Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Produktreferenz-**katalog**

COMPUTERLINKS

Inhaltsverzeichnis

Einleitung 3

GAiA
GAiA 6

Security Gateways
Check Point SecurityPower™ 10
61000 Security System 11
21000 Appliances 13
12000 Appliances 17
IP-Appliances 20
4000 Appliances 23
2200 Appliance 26
Serie 80 Appliances 28
UTM-1 Edge N-Serie Appliances 30
Safe@Office-Appliances 34
SMB Cloud-Managed Security Services 37
DDoS Protector Appliances 39
Zubehör für Check Point-Appliances 2012 41
Virtual Systems 45
Security Gateway Virtual Edition 47
Virtual Appliance für Amazon Web Services 49

Security-Software-Blade-Lösungen

Security Gateway Software Blades
Check Point ThreatCloud™ 52
Firewall Software Blade 53
IPsec VPN Software Blade 55
Mobile Access Software Blade 57
IPS Software Blade 59
Application Control Software Blade 61
URL Filtering Software Blade 62
Anti-Bot Software Blade 63
Antivirus Software Blade 64
Identity Awareness Software Blade 65
Data Loss Prevention Software Blade 66
Data Loss Prevention 68
Web Security Software Blade 68
Antispam & E-Mail Security Software Blade 70
Advanced Networking & Clustering Software Blade 71
Advanced Networking Software Blade 72
Software Blades – Sizing 74

Security Management
Smart-1-Appliances 76
Smart-1 SmartEvent Appliances 78
Network Policy Management Software Blade 80
Endpoint Policy Management Software Blade 82
Logging & Status Software Blade 84
SmartWorkflow Software Blade 86
Monitoring Software Blade 88
Management Portal Software Blade 90
User Directory Software Blade 91
SmartProvisioning Software Blade 92
SmartReporter Software Blade 94
Smart Event Software Blade 96
Multi-Domain Security Management 98

Endpoint Security
Endpoint Security 102
Full Disk Encryption 104
Media Encryption 105
AntiMalware & Program Control 106
Firewall & Compliance Check 108
Remote Access VPN 109
WebCheck 110
Check Point GO 112

Services
Support-Programme und -Pläne von Check Point 116
Check Point Support Timeline 123
Professional Services 129
Schulung und Zertifizierung 130
SmartOptimize 131

Einleitung

DER NEUE PRODUKTREFERENZKATALOG

Willkommen zur neuesten Ausgabe des Check Point-Produktreferenzkatalogs. Der Katalog wurde vollständig von COMPUTERLINKS überarbeitet, um autorisierten Check Point-Partnern einen schnellen und einfachen Überblick über alle wichtigen Informationen zu den Security-Produkten und Lösungen von Check Point zu verschaffen.

TOTAL SECURITY VON CHECK POINT

Der Sicherheitsbereich zeichnet sich durch eine ständig wachsende Komplexität aus. Um dieser Herausforderung zu begegnen, kombiniert die Total Security-Produktreihe von Check Point den Schutz des Netzwerks, den Datenschutz und die Endpunktsicherheit in einer einheitlichen Sicherheitsarchitektur, welche die Sicherheitsprozesse vereinfacht und ein unerreichtes Sicherheitsniveau bietet. Diese einheitliche Sicherheitsarchitektur umfasst folgende Bestandteile:

- Security-Gateways, welche bei höchster Flexibilität und Erweiterbarkeit die umfassendste Sicherheit bieten und gleichzeitig sämtliche Sicherheitsvorgänge einfach und kostengünstig halten
- Den ersten und einzigen Single Endpoint Security Agent, der eine umfassende Lösung für sämtliche Anforderungen der Endgerätesicherheit bietet
- Sicherheitsmanagementlösungen, welche die Konfiguration und Überwachung von Richtlinien sowie die Berichterstellung und die Verwaltung von Sicherheitsereignissen in einer einzigen intuitiven Oberfläche zusammenfassen – und dadurch die Gesamtbetriebskosten reduzieren

Total Security von Check Point baut auf einem einheitlichen Managementansatz auf. Dadurch wird für Unternehmen die Implementierung, die Überwachung sowie die Verwaltung von Netzwerkschutz, Datenschutz und Endpunktsicherheit spürbar einfacher.

SOFTWARE BLADE-ARCHITEKTUR VON CHECK POINT

Mit der Einführung der Software Blade-Architektur stellt Check Point erneut seine Innovationsfähigkeit unter Beweis. Hierbei handelt es sich um eine sichere, flexible und erweiterbare Sicherheitslösung, die vollständig anpassbar ist, so dass sie in jedem Unternehmen und jeder Umgebung die aktuellen Sicherheitsanforderungen exakt erfüllt. Sie stellt die perfekte Alternative zum Einsatz getrennter, eigenständiger Sicherheitssysteme dar.

Diese einzigartige Architektur basiert auf unabhängigen Sicherheitsmodulen, die alle auf einer einzigen Plattform ausgeführt werden, was die Integration und die Verwaltung vereinfacht. Unternehmen können die Sicherheitskonfigurationen so anpassen, dass sie die gewünschte Balance zwischen Schutz und Investitionen erreichen. Gleichzeitig bewahren sie ihre Flexibilität, da die Systeme bei Bedarf später problemlos konsolidiert, neu zugeordnet und ausgebaut werden können. Zusätzlich können die Software Blades auch über jedes beliebige Gateway oder Managementsystem mit einem simplen Mausklick aktiviert und konfiguriert werden – es sind keinerlei Hardware-, Firmware- oder Treiberaktualisierungen erforderlich.

Einleitung (Fortsetzung)

EINHEITLICHE SICHERHEITSARCHITEKTUR VON CHECK POINT

Alle diese Lösungen beruhen auf der einheitlichen Sicherheitsarchitektur von Check Point, die für eine konsistente und effiziente Kontrolle der Sicherheitsinfrastruktur zur Erhöhung der Sicherheit, Reduzierung der Komplexität sowie Senkung der Gesamtbetriebskosten sorgt. Dank unseres breiten Angebots an Produkten und Diensten sind Sie als Check Point-Partner in der Lage, Ihren Kunden eine umfassende End-to-End-Sicherheitslösung zur Verfügung zu stellen, die äußerst effektiv und gleichzeitig leicht zu verwalten und zu kontrollieren ist. Sie können diese Lösungen mit der Gewissheit anbieten, dass es sich dabei um die derzeit modernsten Sicherheitstechnologien handelt, die sich bereits in den weltweit anspruchsvollsten Netzwerkumgebungen bewährt haben.

Wir hoffen, dass Ihnen dieser Katalog von Nutzen ist und Sie bei Ihren Erfolgen unterstützt. Ausführlichere Informationen zu unseren Check Point-Produkten erhalten Sie auf unserer Partner-MAP-Website https://usercenter.checkpoint.com/usercenter oder bei Ihrem regionalen Check Point-Vertreter.

Beachten Sie bitte, dass dieser Katalog nur für Check Point-Partner und nicht für Endkunden vorgesehen ist. Verweisen Sie Kunden, die sich für unsere Check Point-Produkte und -Dienste interessieren, auf die Hersteller-Website www.checkpoint.com.

Check Point GAiA

Das neue einheitliche Betriebssystem von Check Point

GAiA

Das neue Check Point 64-Bit-Betriebssystem

ÜBERSICHT

Check Point GAiA™ ist das innovative und sichere Betriebssystem für alle Check Point Appliances, offene Server und virtualisierte Gateways. GAiA verbindet die leistungsfähigsten Funktionen von IPSO und SecurePlatform in einem einheitlichen Betriebssystem, das für mehr Effizienz und stabile Leistung sorgt. Bei Unterstützung aller Software Blades profitieren Check Point-Kunden mit einer GAIA-Installation von einer verbesserten Verbindungskapazität und dem vollständigen Leistungsspektrum der Sicherheitstechnologie von Check Point.

VORTEILE

- Eine Kombination der leistungsfähigsten Funktionen von IPSO und SecurePlatform
  - Sichere Plattform für alle Check Point-Gateways und Check Point Management, für offene Server und virtualisierte Gateways
  - Unterstützt die gesamte Palette an Software Blades auf allen Check Point-Appliances inkl. der IP-Serie
  - Vollständig kompatibel mit dem IPSO- und SPLAT-Command-Line-Interface
- Erhöhte Betriebseffizienz bei großer Auswahl an Funktionen
  - Intuitive Weboberfläche mit großer Funktionsvielfalt zur Konfiguration und Verwaltung des gesamten Gateways
  - Rollenbasierte Administration ermöglicht Aufgabentrennung anhand unterschiedlicher Benutzerberechtigungen
  - Automatische Durchführung von System-Updates durch neues Software-Update-Tool
  - Wiederherstellen der Gateway-Einstellungen oder Image-Erstellung innerhalb von Minuten
  - Schnelle und effiziente Installation, Sicherung und Wiederherstellung
- Sichere Plattform für die anspruchsvollsten Umgebungen
  - Hohe Verbindungskapazität auf Basis eines 64-Bit-Betriebssystems, das bis zu 70 Millionen gleichzeitige Verbindungen erlaubt
  - Erweiterte Routing-Optionen inkl. ClusterXL und VRRP-Clustering, fünf dynamische Routing-Protokolle und sechs Multicast-Protokolle

INTERESSANT FÜR

- Alle Check Point-Kunden
- IPSO-Kunden, die z.B. das Mobile Access Blade einsetzen wollen
- Kunden, die bisher gemischte SPLAT- und IPSO-Umgebungen warten mussten
- Kunden, die die volle Leistungsfähigkeit Ihrer Hardware nutzen wollen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- 64-Bit-Betriebssystem
- Läuft auf allen Check Point-Appliances (inkl. IP-Serie) und Open Servern
- Unterstützung aller Check Point Software und Service Blades
- Einmalige Kombination von Flexibilität und Simplizität
- Voller IPv4 und IPv6 Support

LEISTUNGSMERKMALE

- Webbasierte Benutzeroberfläche mit Suchnavigation

  Diese Schnittstelle bietet alle Verwaltungsfunktionen in einem webbasierenden Dashboard, auf das über die gängigsten Browser (Internet Explorer, Chrome, Firefox und Safari) zugegriffen werden kann. Die integrierte Suchnavigation liefert sofort Ergebnisse zu Befehlen und Eigenschaften. Für CLI-Benutzer ist das Popup-Fenster mit Shell-Emulator nur einen Klick entfernt.
- Vollständige Software Blade-Unterstützung

  Vordefinierte Lösungspakete sorgen bei unterschiedlichsten Bereitstellungsszenarios für sofortige Sicherheit. Die Software Blades können alternativ bzw. zusätzlich einzeln ausgewählt werden, um dem individuellen Sicherheitskonzept des Unternehmens zu entsprechen.
- Hohe Verbindungskapazität

  Durch den effizienten Einsatz eines 64-Bit-Betriebssystems kann GAiA die Verbindungskapazität Ihrer vorhandenen Check Point-Appliances um ein Vielfaches erweitern.
- Rollenbasierter Administrationszugriff

  Die rollenbasierte Administration gehört zu einer erfolgreichen Sicherheitsrichtlinie und steigert die Betriebseffizienz. Dieser Ansatz bietet GAiA-Kunden die Möglichkeit und Genauigkeit, um Sicherheitsrichtlinien exakt dem Unternehmensbedarf anzupassen. Die Benutzerauthentifizierung und -autorisierung basieren auf den Standardprotokollen RADIUS und TACACS+. Je nach der individuellen Rolle und Verantwortlichkeit können unterschiedliche Zugriffsebenen und somit eine sicherere Umgebung gewährt werden.
- Intelligente Software-Updates

  Die Aktualisierungsdauer wurde auf wenige Sekunden reduziert, und die Suche nach Updates erfolgt nun automatisch. Zu empfohlenen Updates und Status-Meldungen werden Benachrichtigungs-E-Mails versendet. Die Updates können zum automatischen Download und zur Installation während Ruhezeiten eingerichtet werden, sodass Auswirkungen auf Geschäft und Netzwerkressourcen minimiert werden.
- Systemeigener IPv4- und IPv6-Support

  Da sich die Anzahl der verfügbaren IPv4-Adressen immer weiter verringert, wird es zunehmend wichtiger, Ihr Netzwerk für die Umstellung auf IPv6 vorzubereiten. Check Point GAiA ist mit diesen neuen Internetprotokolladressen kompatibel. Support für IPv6 ist im Acceleration und Clustering Blade integriert. Kunden, die zu IPv6 wechseln, profitieren von den in GAiA bereitgestellten Übergangsmethoden Dual Stack und Tunneling.

GAiA

Das neue Check Point 64-Bit-Betriebssystem

- ClusterXL oder VRRP-Cluster

  Mit GAiA können Sie Ihre Plattform frei wählen, egal ob Sie als Redundanzprotokoll die Check Point ClusterXL-Technologie oder das herkömmliche VRRP-Protokoll bevorzugen. Sowohl ClusterXL als auch VRRP werden von GAiA vollständig unterstützt. GAiA ist für alle Check Point-Appliances, offenen Server und virtuellen Umgebungen verfügbar. Es müssen also keine Kompromiss-entscheidungen mehr zwischen den erforderlichen Netzwerkprotokollen und den bevorzugten Sicherheitsplattformen und -funk-tionen getroffen werden.

- Suite für verwaltbares dynamisches Routing

  Die wichtigsten Protokolle, die mit GAiA unterstützt werden, sind:

  Protokolle für dynamisches Routing:
  - RIP RFC 1058
  - RIP Version 2 (mit Authentifizierung) RFC 1723
  - OSPFv2 RFC 2328
  - OSPF NSSA RFC 3101
  - BGP4 RFCs 1771, 1963, 1966, 1997, 2918

  Multicast-Protokolle:
  - IGMPv2 RFC 2236
  - IGMPv3 RFC 3376
  - PIM-SM RFC 4601
  - PIM-SSM RFC 4601
  - PIM-DM RFC 3973
  - PIM-DM state refresh draft-ietf-pim-refresh-02.txt

- Vollständig kompatibel mit IPSO- und SPLAT-CLI-Befehlen

  Der Wechsel zu GAiA ist für Sicherheitsadministratoren praktisch ein Kinderspiel. Die gleichen wirksamen CLI-Befehle (Command Line Interface) von IPSO und SPLAT sind nahtlos in GAiA integriert. Zusätzlich werden weitere neue Befehle und Funktionen der GAiA-CLI hinzugefügt, mit denen die leistungsstarke Command Line Interface noch intuitiver zu bedienen ist.

GAiA Migration: Neue Vorteile von GAiA für bestehende SecurePlatform- und IPSO-Benutzer

Für IPSO-Benutzer:	Für SecurePlatform-Benutzer:
■ Einfache Verwendung • Konfigurationsassistenten • Installation in einem Schritt • Registrierung mit einem Klick	■ Leistungsstarkes Management • Weboberfläche und Befehlszeilenschnittstelle • Rollenbasierte Administration • Konfigurationssätze
■ Vollständige Software Blade-Unterstützung	■ Verwaltbares dynamisches Routing
■ Höhere Verbindungskapazität • 64-Bit-Betriebssystem	■ Höhere Verbindungskapazität • 64-Bit-Betriebssystem
■ IPv6-Sicherheit • Unterstützt Dual Stack und Tunneling • Beschleunigung mit SecureXL und CoreXL	■ IPv6-Sicherheit • Unterstützt Dual Stack und Tunneling • Beschleunigung mit SecureXL und CoreXL
■ Einfache Verwendung • Konfigurationsassistenten • Installation in einem Schritt • Registrierung mit einem Klick	■ Einfache Verwendung • Konfigurationsassistenten • Installation in einem Schritt • Registrierung mit einem Klick
■ Weitere Clustering-Optionen • ClusterXL oder VRRP	■ Weitere Clustering-Optionen • ClusterXL oder VRRP
■ Verbessertes Gerätemanagement • Image-Momentaufnahme (Snapshot) • Geräte-Replikation	■ Verbessertes Gerätemanagement • Image-Momentaufnahme (Snapshot) • Geräte-Replikation
■ Automatisierte Software-Updates	■ Automatisierte Software-Updates

UPGRADE

Upgrade von SecurePlatform

1. Aktualisieren Sie die Produktlizenzen auf R75 oder höher.
2. Schließen Sie ein DVD-Laufwerk über den USB-Port des Computers an.
3. Starten Sie: # patch add cd
4. Wählen Sie die entsprechende Upgrade-Option aus.
5. Nehmen Sie nach dem Upgrade die DVD aus dem Laufwerk.
6. Führen Sie einen Neustart aus.
7. Installieren Sie eine Richtlinie.

Upgrade von IPSO

1. Mounten Sie die GAiA ISO auf einem FTP-Server.
2. Installieren Sie das GAiA-Upgrade-Paket auf der IP-Appliance.
3. Führen Sie das Upgrade-Paket aus.
4. Geben Sie den Speicherort der Sicherung an (optional).
5. Upgrade-Vorlage angeben (Optional)
6. Bestätigen Sie den Vorgang.
7. Das Skript wird automatisch ausgeführt.

ERSTINSTALLATION

Möglichkeit verschiedenster Installations-Optionen wie z.B. per USB-Stick Starten des „First Time Installation Wizard“ über die **Weboberfläche** bzw. **Command Line Interface** oder Erstellen einer Antwortdatei, um den Assistenten unbeaufsichtigt auszuführen.

GESPRÄCHSEINSTIEG

- Verwalten Sie in Ihrer Check Point-Umgebung derzeit unterschiedliche Betriebssysteme (IPSO, SPLAT)?
- Setzen Sie auf IP-Appliances und wollen das volle Spektrum der Check Point Blades setzen?
- Sind Sie an einem 64-Bit-Betriebssystem interessiert?

Check Point
Security Gateways

SecurityPower™

Data Center

Large Enterprise

Medium-Sized Business

Small Business & Branch Office

Dedicated Appliance

2012 Appliance Accessories Guide

Virtualized

Check Point SecurityPower™

Appliances

Der neue Weg, die tatsächliche Leistung von Security Appliances zu messen

Bislang war die Wahl der richtigen Security Appliance für einen spezifischen Einsatzbereich eine große Herausforderung. Unternehmen können sehr unterschiedliche Anforderungen an die Absicherung ihrer Rechnerumgebungen haben: Die Netzwerkgröße, der geforderte Durchsatz, die gewünschten Security-Funktionen, die Fähigkeit, mit künftigem Wachstum Schritt halten zu können oder das bewilligte Budget – all dies sind signifikante Komponenten des Entscheidungsprozesses. Viele Anbieter aber bewerben ihre Lösungen mit einer System-Performance, die lediglich unter Nutzung der Firewall-Security, einer einzigen Firewall-Policy und dazu noch in einer spezifischen Testlaborumgebung gemessen wurde. Im realen Netzwerkverkehr einer Organisation weicht die Appliance-Performance jedoch deutlich von solchen Ergebnissen ab, die unter derart vereinfachten Laborbedingungen erzielt wurden. Die Aufgabe, die richtige Appliance für Ihre Umgebung zu wählen, ist entsprechend schwer zu lösen.

Check Point SecurityPower adressiert die Herausforderung, die passenden Appliances für Ihre spezifischen Anforderungen auszuwählen. Es ist eine neue Metrik, die dem Kunden ermöglicht, Security Appliances nach ihrer Fähigkeit auszuwählen, verschiedene Security-Funktionen und eine typische Security-Policy unter realen Netzwerkbedingungen auszuführen. Jede Appliance hat eine bestimmte SecurityPower-Kapazität SecurityPower Unit, SPU), die ihre Leistung bei der Ausführung mehrerer, fortschrittlicher Security-Funktionen mit einer typischen Security-Policy indiziert.

Die SecurityPower-Kapazität wird bestimmt durch einen Mix aus vielen Performance-Messungen in realen, unterschiedlichen Netzwerken – ein Ergebnis aus umfassenden Datenverkehrsanalysen bei einer großen Anzahl von Check Point-Kunden. Dabei werden verschiedene Kombinationen aus fortschrittlichen Security-Funktionen wie Firewall, IPS, Application Control, Antivirus/Anti-Malware, URL-Filtering und Data Loss Prevention auf das Netzwerk angewendet, und zwar in Verbindung mit einer realistischen Security-Policy, die 100 Firewall-Regeln, Logging für alle Verbindungen, NAT, ein starkes IPS-Schutzprofil und aktuelle Antivirus-Signaturen umfasst. Auf dieser Basis sind Sie in der Lage, Ihre spezifischen Security-Anforderungen bezüglich der erforderlichen SecurityPower-Kapazität zu messen und sie dann mit der für jede Appliance ausgewiesenen Kapazität zu vergleichen – die Appliance-Auswahl wird also deutlich vereinfacht.

SecurityPower ist eine revolutionäre, neue Metrik für die Spezifikation der tatsächlichen Performance und Kapazitäten von Security-Appliances in realen Einsatzszenarien. Mit Hilfe von SecurityPower als Benchmark können Kunden erstmals auf einfache Weise feststellen, welche Security Appliances am besten geeignet sind, ihre aktuellen und auch künftigen, spezifischen Anforderungen an den Schutz des Unternehmensnetzwerks zu erfüllen. Die Auswahl der richtigen Appliance muss nicht länger auf Basis riskanter Mutmaßungen getroffen werden. SecurityPower bietet einen systematischen und wissenschaftlich fundierten Weg für die Berechnung und Bestimmung der optimalen Appliance-Auswahl für eine bestimmte Security-Umgebung.

Für weitere Informationen:

www.checkpoint.com/products/securitypower

61000 Security System

Multi-Blade-basierte Hardware für höchste Sicherheitsansprüche

ÜBERSICHT

Für den Schutz der wohl anspruchsvollsten Netzwerkumgebungen in Rechenzentren sowie bei Telekommunikations- und Cloud Service-Anbietern sind Security und Performance zwei erfolgskritische Faktoren, bei denen keine Kompromisse gemacht werden können. Die Multi-Blade Hardware- und Software-Architektur im 61000 Security System ist ideal für diese Umgebungen. Die Plattform bietet einen skalierbaren Firewall-Durchsatz von 40 bis 200 Gbps und von 3.000 bis 14.600 SecurityPower Units über zwei bis zwölf Security Gateway-Module hinweg in einer Plattform, die auf eine Leistung von bis zu 1 Tbps ausgelegt ist. Das System unterstützt bis zu 70 Millionen gleichzeitiger Verbindungen und 600.000 Sessions pro Sekunde – und bietet damit für Multi-Transaktionsumgebungen eine unvergleichliche Security-Performance.

Das 61000 Security System ist von Grund auf für den Support der hohen Anforderungen von Rechenzentren und Service Providern an hohe Zuverlässigkeit, Verfügbarkeit und Betriebsfähigkeit konzipiert. Das ATCA-Chassis der Carrier-Klasse führt Check Point ClusterXL™ im Hochverfügbarkeits- und Load Sharing-Modus zwischen den Security Gateway-Modulen in einem Chassis aus. Check Point SyncXL™ ermöglicht die hoch effiziente Synchronisation von System- und Security-Informationen zwischen den Komponenten und stellt so eine hohe System-Performance sicher. Durch Hinzufügen eines weiteren 61000 Chassis, das im Hochverfügbarkeitsmodus operiert, wird die Redundanz weiter erhöht und erfolgskritische Aktiva sind zu jeder Zeit verfügbar und geschützt.

Darüber hinaus schützen bewährte, fortschrittliche Security-Technologien von Check Point mit einer Rekord-IPS-Performance von 85 Gbps (im Standard-Profil) oder 40 Gbps (im empfohlenen Security-Profil und bei einem realen Daten-Mix-Aufkommen) selbst vor sehr ausgeklügelten Attacken. Mit dem 61000 Security System können Anwenderunternehmen jede beliebige Anzahl von Security-Vorrichtungen, die in Check Points Software Blade-Architektur verfügbar sind – z. B. Firewall, IPsec VPN, IPS, URL Filtering, Antivirus und Application Control – auf einfache Weise in nur eine integrierte Lösung optimieren und konsolidieren.

VORTEILE

- Bahnbrechende Performance für die anspruchsvollsten Umgebungen
- Vollständige System Redundanz und Betriebsfähigkeit für optimale Verlässlichkeit
- Extrem flexible Hardware-Architektur mit modularen Komponenten
- Automatisches Load-sharing und Load-Balancing zwischen den installierten Komponenten
- Carrier-geeignet mit NEBS L3- und ETSI-Compliance
- 1 Tbps betriebsbereit
- Entwickelt für schnelle Einsatzbereitschaft in weniger als 30 Minuten

LEISTUNGSMERKMALE

- 14600 SecurityPower™
- Hochleistungsfähige, skalierbare Sicherheitslösung mit bis zu 200 Gbps Firewall-Durchsatz
- Hohe Portdichte mit bis zu 32 x 10-GbE-Ports (SFP+), 4 x 40-GbE-Ports (QSFP)
- Intra-/Dual-Chassis-Redundanz
- SNMP-basierte Geräteüberwachung
- Rollenbasierte Administration
- ATCA-kompatibles Chassis der Carrier-Klasse

INTERESSANT FÜR

- Große Rechenzentrumsbetreiber
- Internet Service-Provider
- Carrier und Telefongesellschaften

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Überragende Performance

- 3.000–14.600 SecurityPower™ Units (SPU)
- Bis zu 200 Gbps Firewall-Durchsatz
- Bis zu 85 Gbps IPS-Durchsatz
- Bis zu 600.000 Verbindungen pro Sekunde
- Bis zu 70 Millionen gleichzeitige Verbindungen
- Hohe Portdichte (32 x 10 GbE- oder 4 x 40 GbE-Ports)
- Mehr als 1 Tbps Kapazität und 1,5 Mio. Sessions/s sofort verfügbar

Umfassende und bewährte Sicherheit

- Kompletter Schutz durch die Check Point Software Blade-Architektur
- Bewährte Sicherheit, die bei allen Fortune-100-Unternehmen zum Einsatz kommt
- Einziger Anbieter mit Next-Gen-Firewall und IPS-Zertifizierung durch NSS

Optimierte Verfügbarkeit, Stabilität und Wartbarkeit

- Vollständig redundante Hardware-Systemarchitektur
- Einfache Wartung durch modulare Hot-Swap-Systemkomponenten
- Integrierte Technologie zur Lastverteilung/Lastausgleich
- Check Point ClusterXL und SyncXL für systemübergreifende Lastverteilung/Lastausgleich

Flexibilität und Erweiterbarkeit

- Modulares Design mit Hot-Swap-fähigen Komponenten
- Erweiterbarkeit von 2 auf 12 Gateway-Modulen
- Erweiterbarkeit durch Check Point Software-Blades

61000 Security System

Multi-Blade-basierte Hardware für höchste Sicherheitsansprüche

HARDWARE-SPEZIFIKATIONEN

Sicherheitssystem	61000
10GBase-F SFP+ Ports	12 bis 32
40Base-F QSFP Ports	bis zu 4
SecurityPower[1]	3.000–14.600
Firewall-Durchsatz	bis zu 200 Gbps
IPS-Durchsatz (Standard / empfohlenes Profil)	bis zu 110 Gbps / bis zu 40 Gbps
Concurrent Sessions	bis zu 70 Mio.
Verbindungen pro Sekunde	bis zu 600.000
Sicherheitsswitch-Module	2
Gateway-Module	2 bis 12
Chassi-Management-Module	1 bis 2
Redundante, Hot-Swap-fähige Netzteile	5 AC oder 2 DC
Gehäusetyp	14 U / 15 U*
Abmessungen (Zoll)	17,5“ × 15,16“ × 24,3" (B × T × H)
Abmessungen (metrisch)	445 mm × 385 mm × 618,3 mm (B × T × H)
Gewicht (Chassis, 5 PSUs, Lüfter, 2 CCM)	38 kg
Gewicht (Chassis, 5 PSUs, Lüfter, 2 CCM, 12 SGM, 2 SSM)	90 kg
Betriebsumgebung	Temperatur: -5 bis 55 °C (23 bis 131 °F), Feuchtigkeit: 5 bis 90 % (nicht kondensierend)
Lagerungsumgebung	Temperatur: -40 bis 70 °C (-40 bis 158 °F), Feuchtigkeit: 5 bis 90 % (nicht kondensierend)
Wechselstromversorgung	Anzahl der Module: max. 5 Eingang: 100–240 VAC, 47–63 Hz Leistung: pro Modul 1.200–1.600 W
Gleichstromversorgung	Anzahl der Module: max. 2 Eingang: 48 VDC / 60 VDC, 4 Feeds pro Modul, 50 A/s pro Feed
Zertifizierungen	Sicherheit: CE, UL, TUV Emissionen: CE, FCC Teil 15 Umweltschutz: Kompatibel mit NEBS Level 3, ETSI und RoHS

[1]SecurityPower ist eine revolutionäre, neue Metrik für die Spezifikation der tatsächlichen Performance und Kapazitäten von Security-Appliances in realen Einsatzszenarien. Mit Hilfe von SecurityPower als Benchmark können Kunden erstmals auf einfache Weise feststellen, welche Security Appliances am besten geeignet sind, ihre aktuellen und auch künftigen, spezifischen Anforderungen an den Schutz des Unternehmensnetzwerks zu erfüllen.

*15 U mit Wechselstromversorgung

SOFTWARE-SPEZIFIKATIONEN

Software Blade	61000
Software-Version	R75.x 64-bit
Firewall	■
IPSec VPN	■
Identity Awareness	■
Advanced Networking	■
Acceleration & Clustering	■
IPS	Optional
URL Filtering	Optional
Antivirus & Anti-Malware	Optional
Application Control	Optional

GESPRÄCHSEINSTIEG

- Wie schützen Sie sich vor neuen Bedrohungen?
- Welchen gesetzlichen Bestimmungen und Sicherheitsrisiken stehen Sie heutzutage gegenüber?
- Wie verwalten Sie die wachsenden Sicherheitsanforderungen, die durch soziale Medien wie Facebook, Twitter, YouTube und andere hervorgerufen werden?
- Welche Herausforderung sehen Sie darin, einer Vielzahl von Mobilgeräten den Zugriff auf Ihre Unternehmensdaten zu gestatten?
- Wie können Sie optimale Sicherheit erzielen, ohne das IT-Budget zu überschreiten?

21000 Appliances

Die High-Performance-Rechenzentrumsappliance mit nur 2 Höheneinheiten

ÜBERSICHT

Unter Ausnutzung ihrer Multi-Core- und Beschleunigungstechnologien unterstützt die Check Point 21000 Appliances den schnellsten, am Markt verfügbaren Firewall-Durchsatz von bis zu 110 Gbps und einen IPS-Durchsatz von über 21 Gbps. Die 21000er sind von Grund auf für höchste Flexibilität entwickelt, selbst in den anspruchsvollsten Netzwerkumgebungen großer Organisationen und Rechenzentren.

Die 21000 Appliances bieten, gemessen an wichtigen Investitionskriterien wie Preis pro Port und Preis pro GB, ein herausragendes Preis-Leistungs-Verhältnis, und zwar in einem kleineren Formfaktor, als jedes vergleichbare Konkurrenzprodukt. Die 2-Rack-Unit (2RU) Security Appliance bietet für große Datenpakete einen Durchsatz von mehr als 50 Gbps und unterstützt eine Vielzahl von Kupfer-, Fiberglas-, 1-GbE- und 10-GbE-Netzwerkverbindungen. Eine optionale Beschleunigungskarte wird die Performance der Appliance auf nicht weniger als 110 Gbps und 3.300 SecurityPower Units (SPU) anheben. Optionales Clustering und Komponenten für eine unterbrechungsfreie Betriebsfähigkeit, mit deren Hilfe spielend und ohne jede Serviceunterbrechung Knoten aus dem Cluster entfernt, aktualisiert und wieder eingebracht werden können, befreien die Administration von der Aufgabe, transparente „rolling Upgrades“ durchführen zu müssen.

Für die gesamte Produktfamilie der Check Point Software Blades verfügbar, können die 21000 Appliances bei wachsenden Security-Anforderungen mit zusätzlichen Blades ausgestattet werden. Automatische Updates von Check Point machen die 21000 Appliances zu einer aktiven Security-Lösung, die Ihre Daten, Ihr Netzwerk und Ihre Mitarbeiter auch vor den jüngsten Gefahren und Angriffen schützt.

VORTEILE

- Die leistungsstärkste Security Appliance am Markt in einem kompakten 2U-Chassis
- Maximale Security und Performance für anspruchsvolle RZ-Umgebungen
- Hohe Portdichte unterstützt selbst stark segmentierte Netzwerkumgebungen
- Optimiert für transaktionsorientierte Umgebungen mit geringer Latenzzeit
- Hohe Verfügbarkeit und Betriebsbereitschaft für höchste Zuverlässigkeit
- Einfacher Einsatz und Management von jedem Netzwerk-Standort aus

LEISTUNGSMERKMALE

- 2003 – 3.300 SecurityPower™
- Einfache Bereitstellung und Verwaltung
- Hochverfügbarkeit und einfache Wartung
- Für die Software-Blade-Architektur optimiert
- Niedrige Latenzzeiten
- Hohe Portdichte
- Maximale Sicherheit und Performance

INTERESSANT FÜR

- Hochleistungsumgebungen wie große Standortnetzwerke oder Rechenzentren
- Finanz- und Kommunikationsunternehmen, ISPs, Regierungsbehörden und Produktionseinrichtungen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Überragende Performance

- Bis zu 3.300 SecurityPower™ [1]
- Bis zu 110 Gbps Firewall-Durchsatz [2]
- Bis zu 21 Gbps IPS-Durchsatz [3]
- Maximal 300.000 Verbindungen pro Sekunde [2]
- Bis zu 13 Millionen Verbindungen gleichzeitig
- Geringe Wartezeit mit der Acceleration Card [2]

Umfassende und bewährte Sicherheit

- Kompletter Schutz bei vollständigem Blade Support
- Bewährte Sicherheit, die bei allen Fortune-100-Unternehmen zum Einsatz kommt. Einziger Anbieter mit Next-Gen-Firewall und IPS-Zertifizierung durch NSS

Optimierte Verfügbarkeit, Stabilität und Wartbarkeit

- Maximale Zuverlässigkeit durch redundante Laufwerke, Netzteile und Ventilatoren
- Einfache Wartung mit Hot-Swap-fähigen Netzteilen, Ventilatoren und Laufwerken
- Optimale Systemauslastung mit Check Point ClusterXL für Lastverteilung und Lastausgleich
- Remote-Wiederherstellung über LOM (Light-Out Management)
- Einfacher Zugriff auf wartungsfähige Komponenten ohne Ausbau aus dem Rack

Flexibilität und Erweiterbarkeit

- Große Auswahl an Hardware-Zubehör
- Erweiterbarkeit der Check Point Software-Blades
- Unterstützung von IPv4 und IPv6

21000 Appliances

Die High-Performance-Rechenzentrumsappliance mit nur 2 Höheneinheiten

HARDWARE-SPEZIFIKATIONEN

Appliance	21400	21600
10/100/1000Base-T-Ports	13 bis 37	13 bis 37
1000Base-F SFP-Ports	bis zu 36	bis zu 36
10GBase-F SFP+-Ports	bis zu 12	bis zu 13
SecurityPower[1]	2.003 / 2.900[2]	2.501 / 3.300[2]
Firewall-Durchsatz	50 Gbit/s / 110 Gbit/s[2]	75 Gbit/s / 110 Gbit/s[2]
Firewall-Latenzzeit	< 5 µs[2]	< 5 µs[2]
VPN-Durchsatz	7 Gbit/s / 37 Gbit/s[2]	8,5 Gbit/s / 37 Gbit/s[2]
IPS-Durchsatz (Standard / empfohlenes Profil)	21 Gbit/s / 6 Gbit/s	21 Gbit/s / 6,8 Gbit/s
Concurrent Sessions	10 Mio.[3]	13 Mio.[3]
Verbindungen pro Sekunde	130.000 / 300.000[2]	140.000 / 300.000[2]
VLANs	1.024	1.024
Speicher	12 GB / 24 GB	16 GB / 32 GB
Festplattenspeicher	2 x 500 GB RAID 1	2 x 500 GB RAID 1
E/A-Erweiterungssteckplätze	3	3
Acceleration-Card-Steckplatz	1	1
LOM	Enthalten	Enthalten
Virtual System Unterstützung	Ja	Ja
max. Unterstützte VS (Standard/ max)	125 / 250	150 / 250
Gehäuse	2 U	2 U
Abmessungen (Zoll)	17“ × 28“ × 3,5" (B × T × H)	17“ × 28“ × 3,5” (B × T × H)
Abmessungen (metrisch)	431 mm × 710 mm × 88 mm (B × T × H)	431 mm × 710 mm × 88 mm (B × T × H)
Gewicht	26 kg	26 kg
Betriebsumgebung	Temperatur: 0 bis 40 °C (32 bis 104 °F) Relative Feuchtigkeit 20 bis 90 % (nicht kondensierend)	Temperatur: 0 bis 40 °C (32 bis 104 °F) Relative Feuchtigkeit 20 bis 90 % (nicht kondensierend)
Lagerungsumgebung	Temperatur: -20 bis 70 °C (-4 bis 158 °F) Relative Feuchtigkeit 5 bis 95 % (nicht kondensierend)	Temperatur: -20 bis 70 °C (-4 bis 158 °F) Relative Feuchtigkeit 5 bis 95 % (nicht kondensierend)
Netzeingang	100–240 VAC, 47–63 Hz	100–240 VAC, 47–63 Hz
Spezifikation der Stromversorgung (max.)	2 x 910 W	2 x 1200 W
Stromverbrauch (max.)	449 W	449 W
Zertifizierungen	Sicherheit: UL, cUL Emissionen: CE, FCC Klasse A Umweltschutz: RoHS	Sicherheit: UL, cUL Emissionen: CE, FCC Klasse A Umweltschutz: RoHS

[1] Security Power ist eine revolutionäre, neue Metrik für die Spezifikation der tatsächlichen Performance und Kapazitäten von Security-Appliances in realen Einsatzszenarien. Mit Hilfe von SecurityPower als Benchmark können Kunden erstmals auf einfache Weise feststellen, welche Security Appliances am besten geeignet sind, ihre aktuellen und auch künftigen, spezifischen Anforderungen an den Schutz des Unternehmensnetzwerks zu erfüllen. Die Auswahl der richtigen Appliance muss nicht länger auf Basis riskanter Mutmaßungen getroffen werden.
[2] Mit dem Security Acceleration-Modul
[3] Mit Speicheraufrüstung und Betriebssystem GAiA

21000 Appliances

Die High-Performance-Rechenzentrumsappliance mit nur 2 Höheneinheiten

SOFTWARE-SPEZIFIKATIONEN

Software Blade	21407, 21607	21408, 21608	21409, 21609	21410, 21610	21412, 21612
Software-Versionen	R71.x, R75.x				
Firewall	■	■	■	■	■
Identity Awareness	■	■	■	■	■
IPSec VPN	■	■	■	■	■
Advanced Networking & Clustering	■	■	■	■	■
Mobile Access[1]	■	■	■	■	■
IPS	■	■	■	■	■
Application Control	■	■	Optional	■	■
DLP	Optional	■	Optional	Optional	■
URL Filtering	Optional	Optional	■	■	■
Antivirus	Optional	Optional	■	■	■
Anti-Spam & Email Security	Optional	Optional	Optional	■	■
Anti-Bot	Optional	Optional	■	Optional	Optional
Management Blades					
Network Policy Management	■	■	■	■	■
Logging und Status	■	■	■	■	■
SmartWorkflow	Optional	Optional	Optional	Optional	Optional
Monitoring	Optional	Optional	Optional	Optional	Optional
Management Portal	Optional	Optional	Optional	Optional	Optional
User Directory	Optional	Optional	Optional	Optional	Optional
SmartProvisioning	Optional	Optional	Optional	Optional	Optional
SmartReporter	Optional	Optional	Optional	Optional	Optional
SmartEvent	Optional	Optional	Optional	Optional	Optional
Endpoint Policy Management	Optional	Optional	Optional	Optional	Optional

[1] Fünf Nutzer Lizenzen sind bei der standard Auslieferung enthaltenFive users are included in default package

21000 Appliances

Die High-Performance-Rechenzentrumsappliance mit nur 2 Höheneinheiten

GESPRÄCHSEINSTIEG

- Wie decken Sie den steigenden Bedarf an Durchsatz und Bandbreite ab?
- Wie schützen Sie sich vor neuen Bedrohungen?
- Welchen gesetzlichen Bestimmungen und Sicherheitsrisiken stehen Sie heutzutage gegenüber?
- Wie verwalten Sie die wachsenden Sicherheitsanforderungen, die durch soziale Medien wie Facebook, Twitter, YouTube und andere hervorgerufen werden?
- Welche Herausforderung sehen Sie darin, einer Vielzahl von Mobilgeräten den Zugriff auf Ihre Unternehmensdaten zu gestatten?
- Wie können Sie optimale Sicherheit erzielen, ohne das IT-Budget zu überschreiten?

12000 Appliances

Teilmodulare Appliances für kleine und mittlere Rechenzentren

ÜBERSICHT

Auf Basis ihrer Multi-Core- und Beschleunigungstechnologien bieten die Check Point 12000 Appliances einen schnellen Firewall-Durchsatz von 15 bis 30 Gbps und einen IPS-Durchsatz von 8 bis 17 Gbps. Für die Software-Blade-Architektur optimiert, zielen diese Appliances auf hohe Performance und Zuverlässigkeit selbst in den anspruchsvollsten Unternehmens- und Rechenzentrumsnetzwerken ab.

Die 12000 Appliances bieten, gemessen an wichtigen Investitionskriterien wie Preis pro Port und Preis pro GB, ein herausragendes Preis-Leistungs-Verhältnis, und zwar alle in einem kleineren Formfaktor, als vergleichbare Konkurrenzprodukte. Ob im 1-Rack (1RU)- oder 2-Rack (2RU)-Format, die 12000 Appliances warten mit einer realen Datenverarbeitungsleistung von mehr als 1.800 SecurityPower Units (SPU) und damit einer bislang von keiner anderen Security Appliance dieser Klasse erreichten Performance auf.

Darüber hinaus werden die Geschäftskontinuität und Betriebsfähigkeit durch redundante, hot-swappable Netzanschlüsse und Festplatten sowie ein optionales Lights-out-Management (LOM)-Modul sichergestellt. Damit, und mit den Hochverfügbarkeitsfunktionen in der Software, kann jede potentielle Service-Unterbrechung verhindert oder schnell behoben werden.

VORTEILE

- Rechenzentrumsfähige Security zu attraktiven Preisen
- Flexible Netzwerk-Optionen mit hoher Portdichte für eine Vielzahl verschiedener Netzwerk-Umgebungen
- Leistungsstärkste Security Appliances ihrer Klasse
- Redundante, im Betrieb austauschbare Komponenten stellen die Geschäftskontinuität sicher
- Einfacher Einsatz und zentralisiertes Management von jedem Standort im Netzwerk aus

LEISTUNGSMERKMALE

- 738–1861 SecurityPower™
- 15–30 Gbps Firewall Durchsatz
- 8–17 Gbps IPS Durchsatz
- Redundant ausgelegte Hot-Swap-fähige Netzteile und Speicher
- Lights-Out-Management
- Über drei Erweiterungssteckplätze für bis zu 26 10/100/1000Base-T-Ports oder bis zu 12 1000Base-F (SFP)- bzw. 10Gbase-F (SFP+)-Ports.
- Erweiterte Netzwerksegmentierung mit bis zu 2014 virtuellen LANs (VLAN) Hot-Swap-fähige, redundante Netzteile und die optionalen Clustering- und Wartungskomponenten ermöglichen bei Systemwartungen eine Umverteilung der Arbeitslasten Light-Out Management-Modul (LOM) zur Out-of-Band-Remote-Verwaltung mit Funktionen wie Ferndiagnose und Remote-Neustart der Appliance.
- Zusätzliche Software-Blade-Upgrades sind verfügbar, mit denen Sie Ihre Sicherheitsoptionen erweitern und individuell anpassen können.
- Lokales Management mit einem intuitiven Assistenten zur Ausführung der Erstkonfiguration.

INTERESSANT FÜR

- Hochleistungsumgebungen wie große Standortnetzwerke und Rechenzentren
- Kunden, die kosteneffiziente, erweiterbare Systeme zur Leistungssteigerung benötigen
- Kunden, die Hochleistungs-NGFW und -Netzwerksicherheit benötigen
- Kunden, die höchste Leistung, eine integrierte Firewall und ein integriertes VPN/IPS-Gateway sowie den besten Schutz vor Bedrohungen verlangen
- Finanzdienstleister/Bankinstitute, Gesundheitseinrichtungen, Produktionseinrichtungen, Behörden/Militäreinrichtungen, Kommunikationsunternehmen, Versorgungseinrichtungen und ISP/MSP

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Überragende Performance

- 738–1861 SecurityPower Units
- 15–30 Gbps Firewall-Durchsatz
- 8–17 Gbps IPS-Durchsatz
- 90.000–130.000 Verbindungen pro Sekunde
- 1,2 bis 5 hoch 3 Millionen Verbindungen gleichzeitig

Umfassende und bewährte Sicherheit

- Kompletter Schutz durch die Check Point Software-Blade-Architektur
- Bewährte Sicherheit, die bei allen Fortune-100-Unternehmen zum Einsatz kommt
- Einziger Anbieter mit Next-Gen-Firewall und IPS-Zertifizierung durch NSS

Optimierte Verfügbarkeit und integrierte Sicherheit

- Maximale Zuverlässigkeit durch redundante Laufwerke und Netzteile
- Optimale Systemauslastung mit Check Point ClusterXL für Lastverteilung und Lastausgleich
- Remote-Wiederherstellung über LOM (Light–Out Management)

Flexibilität und Erweiterbarkeit

- Redundante Festplatten und Netzteile
- Große Auswahl an Netzwerkoptionen wie Kupfer, Glasfaser, 1 GbE und 10 GbE
- Unterstützung von IPv4 und IPv6 4
- Fünf dynamische Routing-Protokolle und sechs Multicast-Protokolle

12000 Appliances

Teilmodulare Appliances für kleine und mittlere Rechenzentren

HARDWARE-SPEZIFIKATIONEN

Modell	12200	12400	12600
10/100/1000Base-T-Ports	8 bis 16	10 bis 26	14 bis 26
1000Base-F SFP Ports	0 bis 4	12	12
10GBase-F SFP+ Ports	0 bis 4	12	12
LOM-Karte	Enthalten		
SecurityPower[1]	738	1046	1861
Firewall-Durchsatz	15 Gbps	25 Gbps	30 Gbps
VPN-Durchsatz	2,5 Gbps	3,5 Gbps	7 Gbps
IPS-Durchsatz (Standard / empfohlene Profile)	8 Gbps / 2,5 Gbps	12 Gbps / 3,5 Gbps	17 Gbps / 6 Gbps
Concurrent Sessions	1,2 Mio. / 5,0 Mio.[2]	1,2 Mio. / 5,0 Mio.[2]	1,2 Mio. / 5,0 Mio.[2]
Verbindungen pro Sekunde	90.000	110.000	130.000
VLANS	1024		
Speicher (Basis/Max.)	4 GB / 12 GB	4 GB / 12 GB	6 GB / 12 GB
Festplattenspeicher	1 + 1 500 GB, RAID 1	1 + 1 500 GB, RAID 1	2 500 GB, RAID 1
Gehäusetyp	1 U	2 U	2 U
Abmessungen B × T × H (Zoll)	17,25 × 16,14 × 1,73 Zoll	17,25 × 22,13 × 3,46 Zoll	17,25 × 22,13 × 3,46 Zoll
Abmessungen B×T×H (metrisch)	438 × 410 × 44 mm	438 × 562 × 88 mm	438 × 562 × 88 mm
Gewicht	7,6 kg	23,4 kg	23,4 kg
Betriebsumgebung	Temperatur: 0 bis 40 °C / 32 bis 104 °F, relative Feuchtigkeit 5 bis 90 % (nicht kondensierend)		
Lagerungsumgebung	Temperatur: -20 bis 70 °C / -4 bis 158 °F, relative Feuchtigkeit 5 bis 95 % (nicht kondensierend)		
Redundante, Hot-Swap-fähige Stromversorgung	Optional	Ja	Ja
Netzeingang	100–240 V, 50–60 Hz		
Spezifikation der Stromversorgung (max.)	275 W	300 W	400 W
Stromverbrauch (max.)	121 W	132 W	220 W
Compliance	CB/UL/cUL/CE/FCC/TUV/VCCI/C-Tick		

[1] SecurityPower ist eine revolutionäre, neue Metrik für die Spezifikation der tatsächlichen Performance und Kapazitäten von Security-Appliances in realen Einsatzszenarien. Mit Hilfe von SecurityPower als Benchmark können Kunden erstmals auf einfache Weise feststellen, welche Security Appliances am besten geeignet sind, ihre aktuellen und auch künftigen, spezifischen Anforderungen an den Schutz des Unternehmensnetzwerks zu erfüllen.

[2] Mit Speicheraufrüstung und Betriebssystem GAiA

12000 Appliances

Teilmodulare Appliances für kleine und mittlere Rechenzentren

SOFTWARE-SPEZIFIKATIONEN

Appliance	12207, 12407, 12607	12208, 12408, 12608	12209, 12409, 12609	12210, 12410, 12610
Software-Versionen	R71.x, R75.x			
Firewall	■	■	■	■
Identity Awareness	■	■	■	■
IPSec VPN	■	■	■	■
Advanced Networking & Clustering	■	■	■	■
Mobile Access	■	■	■	■
IPS	■	■	■	■
Application Control	■	■	Optional	■
DLP	Optional	■	Optional	Optional
URL Filtering	Optional	Optional	■	■
Antivirus	Optional	Optional	■	■
Anti-Spam & Email Security	Optional	Optional	Optional	■
Web Security	Optional	Optional	Optional	Optional
Anti-Bot	Optional	Optional	■	Optional
Management Blades				
Network Policy Management	■	■	■	■
Logging und Status	■	■	■	■
SmartWorkflow	Optional	Optional	Optional	Optional
Monitoring	Optional	Optional	Optional	Optional
Management Portal	Optional	Optional	Optional	Optional
User Directory	Optional	Optional	Optional	Optional
SmartProvisioning	Optional	Optional	Optional	Optional
SmartReporter	Optional	Optional	Optional	Optional
SmartEvent	Optional	Optional	Optional	Optional
Endpoint Policy Management	Optional	Optional	Optional	Optional

GESPRÄCHSEINSTIEG

- Wie decken Sie den steigenden Bedarf an Durchsatz und Bandbreite ab?
- Wie schützen Sie sich vor neuen Bedrohungen?
- Welchen gesetzlichen Bestimmungen und Sicherheitsrisiken stehen Sie heutzutage gegenüber?
- Wie verwalten Sie die wachsenden Sicherheitsanforderungen, die durch soziale Medien wie Facebook, Twitter, YouTube und andere hervorgerufen werden?
- Welche Herausforderung sehen Sie darin, einer Vielzahl von Mobilgeräten den Zugriff auf Ihre Unternehmensdaten zu gestatten?
- Wie können Sie optimale Sicherheit erzielen, ohne das IT-Budget zu überschreiten?

IP-Appliances

Flexible Netzwerk- und Leistungsoptionen

IP-Appliances von Check Point, früher bekannt als Nokia IP-Appliances, bieten eine unübertroffene Skalierbarkeit sowie unerreichte Zuverlässigkeit und hohe Portdichte. Sie sorgen so für eine Senkung der Betriebskosten beim Einsatz in anspruchsvollen, geschäftskritischen verteilten Sicherheitsumgebungen. Alle IP-Appliances enthalten Firewall-, IPsec VPN-, IPS-, Advanced Networking- sowie Acceleration & Clustering Software Blades.

Darüber hinaus können Kunden auch zusätzliche Software Blades erwerben, um ihre Sicherheits- und Managementanforderungen zu erfüllen.

IP2455

VORTEILE

- Eine einzige, integrierte Sicherheits-Appliance, die Hardware mit den neuesten Software Blades von Check Point kombiniert
- Dank modularer und skalierbarer Architektur in höchstem Maße erweiterbar und anpassbar, um im gesamten Spektrum der verschiedenen Arten von Datenverkehr höchste Leistung und höchsten Schutz zu bieten
- Bietet geringe durchschnittliche Wartungszeiten und garantiert Zuverlässigkeit durch Wartbarkeit und Redundanz der Carrier-Klasse

LEISTUNGSMERKMALE

- Die erweiterbare, flexible Software-Blade-Architektur bietet unübertroffene Möglichkeiten zur schnellen und problemlosen Erweiterung der Sicherheitsfunktionen durch das Hinzufügen zusätzlicher Software Blades von Check Point und senkt so die Gesamtbetriebskosten und gewährleistet kosteneffizienten Schutz.
- Dank ADP-Modulen (Accelerated Data Path, beschleunigter Datenpfad) kann die CPU-Rechenlast zwischen dem Hauptprozessor und dem ADP-Modul aufgeteilt werden. Dadurch wird die Leistung gesteigert und gleichzeitig Ihre Appliance-Investition geschützt.
- Die erweiterten Routing- und Netzwerkfunktionen unterstützen eine Vielzahl verschiedener Arten von Datenverkehr, darunter PIM, RIP, OSPF sowie BGP, und sie ermöglichen Problembehebung, Kapazitätsplanung und Konfigurationsmanagement von einem entfernten Standort aus.
- Das VRR-Protokoll (VRRP, Virtual Router Redundancy Protocol) und die patentierte IP-Appliance-Clustering-Technologie von Check Point garantieren höchste Leistung und Hochverfügbarkeit.
- Die optionale Clustering-Funktionalität ermöglicht eine Umverteilung der Arbeitslasten, wenn zur Systemwartung Aktualisierungen durchgeführt werden müssen. Dadurch können Administratoren Updates einspielen, ohne die Endanwender in ihrer Arbeit zu unterbrechen.
- Network Voyager ermöglicht die Fernkonfiguration, die Fernüberwachung und das Management aus der Ferne über eine grafische Oberfläche mit großem Funktionsumfang.
- Die Schnittstellenoptionen umfassen Ethernet über Kupferkabel und über Glasfaser, mit einer Vielzahl möglicher Portdichten und Leistungsoptionen bis hin zu 10 Gbit/s und T1WAN.
- Als Speichermöglichkeiten stehen Festplatten, Flash und Hybrid-Lösungen zur Verfügung.

INTERESSANT FÜR

- Kunden, die bereits eine IP-Appliance verwenden und ihre aktuelle Infrastruktur mit möglichst geringen Beeinträchtigungen erweitern oder auf den neuesten Stand bringen wollen
- Kunden, die das gesamte Unternehmen auf eine einheitliche Sicherheitsplattform umstellen wollen – von Rechenzentren bis hin zu Zweigstellen
- Großunternehmen mit einer sich kontinuierlich weiterentwickelnden IT-Infrastrukturumgebung – mit verschiedensten Arten von Internetdatenverkehr, der eine kosteneffiziente, anpassungsfähige Appliance mit einer Vielzahl von Optionen erfordert
- Kunden, die ein umfangreiches Portfolio von E/A-Optionen, hohe Portdichte, Unterstützung einer Vielzahl unterschiedlicher Protokolle oder Wartbarkeit der Carrier-Klasse benötigen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Ermöglicht einfache, erweiterbare Sicherheit und Leistung dank zusätzlicher Software Blades, Beschleunigungstechnologien wie ADP, CoreXL und SecureXL sowie verschiedenster Konnektivitätsoptionen
- Bietet Wartbarkeit und Zuverlässigkeit der Carrier-Klasse
- Bietet stark vereinheitlichte und intuitive Verwaltung
- Bietet höchste Leistung bei höchster Sicherheit

GESPRÄCHSEINSTIEG

- Planen Sie, Ihre Netzwerksicherheit zu erweitern oder auf den aktuellen Stand zu bringen (z. B. Firewall, VPN, IPS) oder weitere DMZs hinzuzufügen?
- (Für Kunden, die bereits eine IP-Appliance einsetzen) Sind Sie zufrieden mit Ihren IP-Appliances?
- Benötigen Sie Multi-Gigabit-Datendurchsatz (d. h. 10-Gbit/s-Schnittstellen), Erweiterbarkeit und Hochverfügbarkeit?
- Benötigen Sie intuitive Administrationsmöglichkeiten und leicht zugängliche Wartungsmöglichkeiten für Ihre Appliances?
- Verfügen Sie über DMZs, die überdurchschnittlichen Transaktionsdatenverkehr oder große Datentransfers aufweisen?

IP-Appliances

Flexible Netzwerk- und Leistungsoptionen

HARDWARE-SPEZIFIKATION FÜR IP-APPLIANCES

	IP282	IP297	IP397	IP567	IP697	IP1287	IP2457
10/100/1000-Ports	6	6/8	4/8	4/12	4/16	4/28	4/32
10-GbE-Ports	-	-	-	-	61	10[1]	10[1]
Festplattenspeicher	40 GB	40 GB	80 GB	80 GB	80 GB	80 GB	80 GB
HDD-basiert oder Flash	HDD	HDD oder Flash	HDD oder Flash	HDD oder Flash	HDD oder Flash	HDD oder Flash	HDD oder Flash
Gehäuse	1 U / Halb-Rack	1 U / Halb-Rack	1 U	1 U	1 U	2 U	2 U
Abmessungen (Zoll)	8,52 × 18 × 1,71 Zoll	8,52 × 18 × 1,71 Zoll	17 × 16 × 1,71 Zoll	17,23 × 22 × 1,71 Zoll	17,23 × 24 × 1,71 Zoll	17,23 × 24,11 × 3,46 Zoll	17,23 × 24,11 × 3,46 Zoll
Abmessungen (metrisch)	216 × 457 × 44 mm	216 × 457 × 44 mm	432 × 406 × 44 mm	438 × 559 × 44 mm	438 × 610 × 44 mm	438 × 613 × 88 mm	438 × 613 × 88 mm
Gewicht	5,1 kg (11,25 lbs)	5,1 kg (11,25 lbs)	7,71 kg (17,0 lbs)	11,84 kg (26,1 lbs)	12,38 kg (27,3 lbs)	19,6 kg (43,2 lbs)	20,57 kg (45,35 lbs)
Betriebsumgebung	Temperatur: 0 bis 40 °C, Luftfeuchtigkeit: 5 bis 95 %, (nicht kondensierend), Höhe: 3.048 m	Temperatur: 5 bis 40 °C[2], relative Luftfeuchtigkeit: 10 bis 85 % (nicht kondensierend), Höhe: 2.500 m					
Lagerungsumgebung	Temperatur: -20°C bis 70°C, relative Luftfeuchtigkeit: 5 bis 95 %						
Netzeingang	100–240 V, 50–60 Hz						
Duale, Hot-Swap-fähige Stromversorgung	Nein	Nein	Nein	Nein	Enthalten	Enthalten	Enthalten
Netzteile (max.)	133 W	133 W	150 W	225 W	250 W	700 W	700 W
Stromverbrauch (max.)			100 W	165 W			
Gleichstromversorgung	-	-	-	-	-	Optional	Optional
Compliance	UL60950-1, Erste Ausgabe: 2003, CAN/CSAC22.2, Nr. 60950:2000, IEC60950-1: 2001, EN60950-1:2001+A11 mit nationalen Abweichungen in Japan / Emissionsgrenzwerte: FCC Teil 15, Subpart B, Klasse A, EN50024, EN55022A: 1998, CISPR 22 Klasse A: 1985, EN61000-3-2, EN61000-3-3 / Widerstandsfähigkeit: EN55024: 1998 ROHS, WEEE						

[1] Optional

[2] IP395 kann bei bis zu 50 °C betrieben werden.

IP-Appliances

Flexible Netzwerk- und Leistungsoptionen

LEISTUNGSDATEN DER IP-APPLIANCES

	IP282	IP297	IP397	IP567	IP697	IP1287	IP2457
SecurityPower[3]	113	113	116	116	268	670	1.112
Firewall-Durchsatz	1,5 Gbit/s	1,5 Gbit/s	3,0 Gbit/s	7 Gbit/s	11,7 Gbit/s[1]	17,5 Gbit/s[1]	30 Gbit/s[1]
Festplattenspeicher	40 GB	40 GB	80 GB	80 GB	80 GB	80 GB	80 GB
VPN-Durchsatz	1,0 Gbit/s	1,0 Gbit/s	677 Mbit/s	1,7 Gbit/s	3,3 Gbit/s	8,3 Gbit/s	8,3 Gbit/s
IPS-Durchsatz	1,4 Gbit/s	1,4 Gbit/s	2,9 Gbit/s	2,9 Gbit/s	4 Gbit/s	7 Gbit/s	9 Gbit/s
Concurrent Sessions	900.000	900.000	1 Mio.	1 Mio.	1 Mio.	1 Mio. / 3,3 Mio.[4]	1 Mio. / 3,3 Mio.[4]
VLANS	1024[2]	1024[2]	1024[2]	1024[2]	1024[2]	1024[2]	1024[2]
ADP-Modul	-	-	-	-	Optional	Optional	Optional
VPN-Beschleunigung	Optional	Optional	■	■	■	■	■

[1] Performance mit ADP
[2] Maximal 256 VLANs pro Schnittstelle
[3] SecurityPower ist eine revolutionäre, neue Metrik für die Spezifikation der tatsächlichen Performance und Kapazitäten von Security-Appliances in realen Einsatzszenarien. Mit Hilfe von SecurityPower als Benchmark können Kunden erstmals auf einfache Weise feststellen, welche Security Appliances am besten geeignet sind, ihre aktuellen und auch künftigen, spezifischen Anforderungen an den Schutz des Unternehmensnetzwerks zu erfüllen.
[4] Mit Speicheraufrüstung und Betriebssystem GAiA

SOFTWARE-SPEZIFIKATION FÜR IP-APPLIANCES

	IP282	IP 295/297		IP 395/397		IP 565/567		IP 695/697		IP 1285/1287		IP 2455/2457	
Software-Version	R65, R70, R71, R75	R65, R70, R71, R75		R65, R70, R71, R75		R65, R70, R71, R75		R65, R70, R71, R75		R65, R70, R71, R75		R65, R70, R71, R75	
Firewall	■	■	■	■	■	■	■	■	■	■	■	■	■
IPsec VPN	■	■	■	■	■	■	■	■	■	■	■	■	■
Application Control	Optional	Optional	■	Optional	■	Optional	■	Optional	■	Optional	■	Optional	■
IPS	Optional	■	■	■	■	■	■	■	■	■	■	■	■
Identity Awareness	Optional	Optional	■	Optional	■	Optional	■	Optional	■	Optional	■	Optional	■
Acceleration & Clustering	Optional	■	■	■	■	■	■	■	■	■	■	■	■
Advanced Networking	Optional	■	■	■	■	■	■	■	■	■	■	■	■
Web Security	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
URL Filtering (ab R75.20)	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Anti-Bot	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
DLP	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Antivirus	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Anti-Spam & Email Security	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional

4000 Appliances

Leistungsfähige Appliances für den Mittelstand

ÜBERSICHT

Angesichts zunehmender Gefahren für die Sicherheit von Daten und Unternehmensnetzen müssen moderne Security Gateways weitaus mehr sein, als „nur" eine Firewall – sie müssen verschiedene Technologien nutzen, um den Netzwerkzugriff zu kontrollieren, ausgeklügelte Attacken zu erkennen und abzuwehren und zusätzliche Funktionalitäten zur Verfügung stellen, wie zum Beispiel für Data Loss Prevention und den Schutz vor Web-basierten Gefahren.

Die Check Point 4000 Appliances verbinden schnelle Netzwerktechnologie mit hoch performanten Multi-Core-Kapazitäten und bieten damit eine beispiellose, vielschichtige Security, ohne jedoch die System-Performance zu beeinträchtigen. Die 4000 Appliances umfassen maximal sechzehn 1-Gigabit-Ethernet-Ports, redundante, im laufenden Betrieb wechselbare (hot swappable) Netzanschlüsse und ein optionales out-of-band LOM (Lights Out Management)-Modul in einem rahmenmontierbaren, kompakten 1U-Format. Mit einem Firewall-Durchsatz von bis zu 11 Gbps, einem IPS-Durchsatz von 6 Gbps und 623 SecurityPower-Units bieten diese Appliances die beste Performance in ihrer Klasse.

Bei Security-Entscheidungen muss nicht länger zwischen Funktionen und Performance gewählt werden. Mit den Check Point 4000 Appliances und der ausbaufähigen Software-Blade-Architektur können die Kunden darauf vertrauen, dass die eingesetzten Security-Lösungen ihren Schutzerfordernissen entsprechen und selbst in den anspruchsvollsten Netzwerkumgebungen die Performance-Anforderungen erfüllen.

VORTEILE

- Kompaktes 1U-Chassis für integrierte Security und Security-Konsolidierung
- Verlässliche, Enterprise-fähige Security Appliance mit Multi-Core-Technologie und Remote-Management-Funktionen
- Flexible Netzwerk-Optionen mit Kupfer-, Fiberglas-, 1GbE- und 10GbE-Ports
- Bewährte und ausbaufähige Security für den Schutz des Perimeters und der Segmente von Unternehmensnetzen
- Einfacher Einsatz und zentralisiertes Management von jeder Stelle im Netzwerk aus

LEISTUNGSMERKMALE

Ein Hochleistungspaket mit kompaktem 1U-Formfaktor

Die Check Point 4000 Appliances kombinieren modernste Multi-core-Technologien mit hohem Netzwerkdurchsatz, um Ihnen ein breites Spektrum an Netzwerksicherheitsoptionen ohne Leistungsverlust anzubieten.

Diese Sicherheits-Appliances können bis zu 623 SecurityPower-Einheiten verarbeiten und bieten einen Firewall-Durchsatz von bis zu 11 Gbps bzw. einen IPS-Durchsatz von bis zu 6 Gbps.

Optimierte Bereitstellung und Verwaltung

Jede Appliance verfügt über ein lokales Management mit einem intuitiven Wizard zur Ausführung der Erstkonfiguration. Mit dem integrierten Management kann man ein weiteres Gateway verwalten, was in einem HA-Szenario sinnvoll sein kann.

Die optionale webbasierte Administration und das zentrale Management über die Security Management Software-Blades von Check Point sorgen für eine schnelle, einfache und sichere Verwaltung von jedem Ort im Netzwerk. Automatische Updates von Check Point halten die 4000 Appliances auf dem neuesten Stand, um jederzeit vor aktuellen Bedrohungen und Exploits zu schützen und bieten so höchste Sicherheit für Ihr Netzwerk, Ihre Daten und Ihre Mitarbeiter.

Flexible Netzwerkoptionen

Die modularen Netzwerkeinschübe ermöglichen den Einsatz in jeder Netzwerkumgebung – acht 1-GbE-Kupferanschlüsse sind enthalten. Sie haben außerdem die Option, acht weitere 1-GbE-Kupferanschlüsse, vier 1-GbE-Glasfaseranschlüsse oder zwei 10-GbE-Glasfaseranschlüsse entsprechend Ihrem Unternehmensbedarf hinzuzufügen.

Die 4000 Appliance unterstützt bis zu 1.024 VLANs für eine höhere Netzwerksegmentierung.

INTERESSANT FÜR

- Kleine bis mittelgroße Unternehmen
- Finanzdienstleister/Bankinstitute, Gesundheitseinrichtungen, Produktionseinrichtungen, Behörden/Militäreinrichtungen, Kommunikationsunternehmen, Versorgungseinrichtungen und ISP/MSP

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Überragende Performance

- 114–623 SecurityPower-Einheiten
- 3–11 Gbps Firewall-Durchsatz
- 2–6 Gbps IPS-Durchsatz
- 25.000–80.000 Verbindungen pro Sekunde
- 1,2 bis 3,3 hoch 3 Millionen Verbindungen gleichzeitig

Bewährte und erweiterbare Sicherheit

- Bewährte Sicherheit, die bei allen Fortune-100-Unternehmen zum Einsatz kommt. Flexible Erweiterung um beliebige Software Blades wie Mobile Access, DLB, Application Control usw.
- NSS-Gütesiegel „Empfohlen" für Firewall, IPS und NGFW

Zuverlässige Enterprise-Klasse

- Optimierte Multicore-Technologie für Software Blades-Architektur
- Inklusive LOM (nur 4800)
- Redundante Netzteile (nur 4800)

Flexible Netzwerkoptionen

- Optionen für Kupfer, Glasfaser, 1 GbE und 10 GbE für den Einsatz in jeder Netzwerkumgebung
- Unterstützung von IPv4 und IPv6
- Fünf dynamische Routing-Protokolle und sechs Multicast-Protokolle

4000 Appliances

Leistungsfähige Appliances für den Mittelstand

HARDWARE-SPEZIFIKATIONEN

Modell	4200	4400	4600	4800
10/100/1000Base-T-Ports	4 bis 8	8 bis 12	8 bis 12	8 bis 16
1000Base-F SFP-Ports	0 bis 4	0 bis 4	0 bis 4	0 bis 4
10GBase-F SFP+-Ports	-	-	-	0 bis 2
SecurityPower[1]	114	223	374	623
Firewall-Durchsatz	3 Gbps	5 Gbps	9 Gbps	11 Gbps
VPN-Durchsatz	400 Mbit/s	1,2 Gbps	1,5 Gbps	2 Gbps
IPS-Durchsatz (Standard / empfohlene Profile)	2 Gbps 0,3 Gbps	3,5 Gbps 0,7 Gbps	4 Gbps 1 Gbps	6 Gbps 1,5 Gbps
Concurrent Sessions	1,2 Mio.	1,2 Mio.	1,2 Mio.	1,2 Mio. / 3,3 Mio.[2]
Verbindungen pro Sekunde	25.000	40.000	50.000	70.000
VLANs	1.024	6 Gbps	130.000	14 bis 26
Speicher	4 GB	4 GB	4 GB	4 GB / 8 GB
Festplattenspeicher	250 GB	4 GB / 12 GB	6 GB / 12 GB	14 bis 26
LOM	-	-	-	Enthalten
Gehäuse	1 U			
Abmessungen B × T × H (Zoll)	17,25 × 12,56 × 1,73 Zoll		17,25 x 16,14 x 1,73 Zoll	
Abmessungen B×T×H (metrisch)	438 × 319 × 44 mm		438 × 410 × 44 mm	
Gewicht	4,0 kg	7,5 kg	7,6 kg	
Betriebsumgebung	Temperatur: 0 bis 40 °C / 32 bis 104 °F, relative Feuchtigkeit 20 bis 90 % (nicht kondensierend)			
Lagerungsumgebung	Temperatur: -20 bis 70 °C / 14 bis 158 °F, relative Feuchtigkeit 5 bis 95 % (nicht kondensierend)			
Redundante, Hot-Swap-fähige Stromversorgung	-	-	-	Optional
Netzeingang	100–240 V, 50–60 Hz			
Spezifikation der Stromversorgung (max.)	100 W	250 W	275 W	
Stromverbrauch (max.)	57 W	90 W	140 W	
Compliance	CB/UL/cUL/CE/FCC/TUV/VCCI/C-Tick			

[1] SecurityPower ist eine revolutionäre, neue Metrik für die Spezifikation der tatsächlichen Performance und Kapazitäten von Security-Appliances in realen Einsatzszenarien. Mit Hilfe von SecurityPower als Benchmark können Kunden erstmals auf einfache Weise feststellen, welche Security Appliances am besten geeignet sind, ihre aktuellen und auch künftigen, spezifischen Anforderungen an den Schutz des Unternehmensnetzwerks zu erfüllen.

[2] Mit Speicheraufrüstung und Betriebssystem GAiA

4000 Appliances

Leistungsfähige Appliances für den Mittelstand

SOFTWARE-SPEZIFIKATIONEN

Appliance	4205	4207 4407 4607 4807	4208 4408 4608 4808	4809	4210 4410 4610 4810
Software-Version	■	■	■	■	■
Firewall	■	■	■	■	■
Identity Awareness	■	■	■	■	■
IPSec VPN	■	■	■	■	■
Advanced Networking & Clustering	■	■	■	■	■
Mobile Access	■	■	■	■	■
IPS	Optional	■	■	■	■
Application Control	Optional	■	■	Optional	■
DLP	Optional	Optional	■	Optional	Optional
URL Filtering	Optional	Optional	Optional	■	■
Antivirus	Optional	Optional	Optional	■	■
Anti-Spam & Email Security	Optional	Optional	Optional	Optional	■
Web Security	Optional	Optional	Optional	Optional	Optional
Anti-Bot	Optional	Optional	Optional	■	Optional
Management Blades					
Network Policy Management	■	■	■	■	■
Logging and Status	■	■	■	■	■
SmartWorkflow	Optional	Optional	Optional	Optional	Optional
Monitoring	Optional	Optional	Optional	Optional	Optional
Management Portal	Optional	Optional	Optional	Optional	Optional
User Directory	Optional	Optional	Optional	Optional	Optional
SmartProvisioning	Optional	Optional	Optional	Optional	Optional
SmartReporter	Optional	Optional	Optional	Optional	Optional
SmartEvent	Optional	Optional	Optional	Optional	Optional
Endpoint Policy Management	Optional	Optional	Optional	Optional	Optional

GESPRÄCHSEINSTIEG

- Wie schützen Sie sich vor neuen Bedrohungen?
- Welchen gesetzlichen Bestimmungen und Sicherheitsrisiken stehen Sie heutzutage gegenüber?
- Welche Herausforderung sehen Sie darin, einer Vielzahl von Mobilgeräten den Zugriff auf Ihre Unternehmensdaten zu gestatten?
- Welches sind die wichtigsten Aspekte, die Sie bei der Auswahl einer Sicherheitsanwendung in Ihre Entscheidung einbeziehen?
- Wie decken Sie den steigenden Bedarf an Durchsatz und Bandbreite ab?
- Wie können Sie optimale Sicherheit erzielen, ohne das IT-Budget zu überschreiten?

2200 Appliance

Appliance für kleine und mittlere Standorte

ÜBERSICHT

Durchgängige Security erfordert nicht nur den Schutz für die wichtigsten Unternehmensnetze – um eine einheitliche und vollständige Abwehr von potentiellen Gefahren zu gewährleisten, muss der gleiche Schutz auch für entfernte Niederlassungen und Zweigstellen gegeben sein. Die Check Point 2200 Appliance ist die ideale Lösung für die Bereitstellung von Security für Kleinbetriebe und Zweigstellen.

Die 2200 Appliance bietet Security auf Enterprise-Niveau bei einem herausragenden Preis-Leistungs-Verhältnis und im kompakten Desktop-Format. Mit ihrer Multi-Core-Technologie, sechs 1-Gigabit-Ethernet-Ports und dem vollständigen Support der Software-Blade-Architektur ermöglicht sie eine natürliche Ausweitung der Unternehmens-Security auf entfernte Zweigstellen. Trotz ihres kleinen Formats bietet diese leistungsstarke Appliance respektable 114 SecurityPower-Units, einen Firewall-Durchsatz von 3 Gbps und einen IPS-Durchsatz von mehr als 2 Gbps. Die Lösung ist ab 3.600.- US-Dollar erhältlich und mit 5, 7, 8 oder 10 Software Blades vorkonfiguriert. Damit ist die 2200 Appliance eine effektive und erschwingliche Security-Lösung im „all-in-one"-Format. Für eine evtl. erforderliche Kapazitätserweiterung und individuelle Schutzoptionen können zusätzliche Software Blades hinzugefügt werden.

VORTEILE

- Bewährte Sicherheit, die bei allen Fortune-100-Unternehmen zum Einsatz kommt
- Einheitliche Management-Oberfläche
- Flexibel erweiterbare Software-Blade-Architektur

LEISTUNGSMERKMALE

- 114 SecurityPower™
- 3 GbpsGbps Firewall-Durchsatz
- 2 Gbps IPS-Durchsatz
- 6 10/100/1000Base-T-Ports
- Desktop-Formfaktor

INTERESSANT FÜR

- Kleine Unternehmen und Zweigestellen, die eine integrierte Security-Lösung benötigen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Überragende Performance

- 114 SecurityPower Units[1]
- 3 Gbps Firewall-Durchsatz
- 2 Gbps IPS-Durchsatz
- 25.000 Verbindungen pro Sekunde
- Bis zu 1,2 Millionen Verbindungen gleichzeitig

Bewährte und erweiterbare Sicherheit

- Bewährte Sicherheit, die bei allen Fortune-100-Unternehmen zum Einsatz kommt. Flexible Ergänzung um weitere Blades wie Mobile Access, DLP, Application Control usw. möglich
- Einziger Anbieter mit Next-Gen-Firewall und IPS-Zertifizierung durch NSS

Einfache und schnell bereitzustellende Komplettlösung

- Vorinstallierte Software Blades auf einer Appliance der Enterprise-Klasse
- Integriertes lokales Management

GESPRÄCHSEINSTIEG

- Wie schützen Sie sich vor neuen Bedrohungen?
- Welchen gesetzlichen Bestimmungen und Sicherheitsrisiken stehen Sie heutzutage gegenüber?
- Welche Herausforderung sehen Sie darin, einer Vielzahl von mobilen Endgeräten den Zugriff auf Ihre Unternehmensdaten zu gestatten?
- Welches sind die wichtigsten Aspekte, die Sie bei der Auswahl einer Sicherheitsanwendung in Ihre Entscheidung einbeziehen?
- Wie decken Sie den steigenden Bedarf an Durchsatz und Bandbreite ab?
- Wie können Sie optimale Sicherheit erzielen, ohne das IT-Budget zu überschreiten?

2200 Appliance

Appliance für kleine und mittlere Standorte

HARDWARE-SPEZIFIKATIONEN

Modell	2200
10/100/1000Base-T-Ports	6
SecurityPower[1]	114
Firewall-Durchsatz	3 Gbps
VPN-Durchsatz	400 Mbit/s
IPS-Durchsatz (Standard / empfohlene Profile)	2 Gbps / 0,3 Gbps
Concurrent Sessions	1,2 Mio.
Verbindungen pro Sekunde	25.000
VLANs	1.024
Festplattenspeicher	250 GB
Gehäuse	Desktop
Abmessungen (Zoll)	8,27“ × 8,25“ × 1,65" (B × T × H)
Abmessungen (metrisch)	210 mm × 209 mm × 42 mm (B × T × H)
Gewicht	2 kg
Betriebsumgebung	Temperatur: 0 bis 40 °C / 32 bis 104 °F Relative Feuchtigkeit 5 bis 90 % (nicht kondensierend)
Lagerungsumgebung	Temperatur: -4 bis 70 °C / -20 bis 158 °F Relative Feuchtigkeit 5 bis 95 % (nicht kondensierend)
Netzeingang	100–240 V, 50–60 Hz
Spezifikation der Stromversorgung (max.)	40 W
Stromverbrauch (max.)	35 W
Compliance	Sicherheit: UL, cUL Emissionen: CE, FCC Klasse A, VCCI, C-Tick Umweltschutz: RoHS

[1] SecurityPower ist eine revolutionäre, neue Metrik für die Spezifikation der tatsächlichen Performance und Kapazitäten von Security-Appliances in realen Einsatzszenarien. Mit Hilfe von SecurityPower als Benchmark können Kunden erstmals auf einfache Weise feststellen, welche Security Appliances am besten geeignet sind, ihre aktuellen und auch künftigen, spezifischen Anforderungen an den Schutz des Unternehmensnetzwerks zu erfüllen.

HARDWARE-SPEZIFIKATIONEN

Appliance	2205	2207	2208	2210
Software-Versionen	R71.x, R75.x			
Firewall	■	■	■	■
Identity Awareness	■	■	■	■
IPSec VPN	■	■	■	■
Advanced Networking & Clustering	■	■	■	■
Mobile Access	■	■	■	■
IPS	Optional	■	■	■
Application Control	Optional	■	■	■
DLP	Optional	Optional	■	Optional
URL Filtering	Optional	Optional	Optional	■
Antivirus	Optional	Optional	Optional	■
Anti-Spam & Email Security	Optional	Optional	Optional	■
Web Security	Optional	Optional	Optional	Optional
Anti-Bot	Optional	Optional	Optional	Optional
Management Blades				
Network Policy Management	■	■	■	■
Logging and Status	■	■	■	■
SmartWorkflow	Optional	Optional	Optional	Optional
Monitoring	Optional	Optional	Optional	Optional
Management Portal	Optional	Optional	Optional	Optional
User Directory	Optional	Optional	Optional	Optional
SmartProvisioning	Optional	Optional	Optional	Optional
SmartReporter	Optional	Optional	Optional	Optional
SmartEvent	Optional	Optional	Optional	Optional
Endpoint Policy Management	Optional	Optional	Optional	Optional

Serie 80 Appliances

Vollständige All-inclusive-Sicherheit für kleinere Zweigstellen

ÜBERSICHT

Die Serie-80-Appliances von Check Point sind komplett ausgestattete, zentral verwaltete Sicherheits-Appliances für Zweigstellen und externe Standorte. Sie basieren auf den gleichen erstklassigen Technologien von Check Point, die von sämtlichen Fortune-100-Unternehmen eingesetzt werden.

Serie-80

VORTEILE

- Die Appliances der Serie 80 von Check Point setzen durch die Erweiterung der Software Blades bis hin zum äußersten Rand des Netzwerks neue Maßstäbe in puncto Sicherheit für Zweigniederlassungen und bieten als bisher einziges System der Branche Sicherheit der Enterprise-Klasse im kleinsten Desktop-Formfaktor

LEISTUNGSMERKMALE

- Firewall-Durchsatz: max. 1,5 Gbit/s (große Datenpakete)
- VPN-Durchsatz: max. 220 Mbit/s (große Pakete)
- IPS-Durchsatz: max. 720 Mbit/s
- AV-Durchsatz: max. 100 Mbit/s
- Gleichzeitige Sessions: 150.000

INTERESSANT FÜR

- Unternehmen mit mehreren Zweigniederlassungen, die zentral verwaltete, sichere Konnektivität zwischen den Niederlassungen und zum Internet benötigen
- Vertikale Schlüsselbranchen: Einzelhandel, Gesundheitswesen, Finanzdienstleistungen und Versicherungen
- Service Provider, die Managed Services für Unternehmen mit mehreren Zweigniederlassungen anbieten

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Hervorragendes Preis-Leistungs-Verhältnis
- Dank hoher Portdichte werden in kleinen Zweigniederlassungen keine zusätzlichen Switch-Ports benötigt
- Bietet umfassende und erweiterbare Sicherheit mittels Software Blades
- Erweitert den Funktionsumfang ganz nach Bedarf mit der Software-Blade-Architektur
- Bringt Sicherheits-Software-Management der Enterprise-Klasse von der Unternehmenszentrale in die Zweigniederlassungen
- Einfache Bereitstellung ganz ohne Unterstützung der Unternehmens-IT

GESPRÄCHSEINSTIEG

- Wie viele verschiedene Geräte sind gegenwärtig in Ihren Zweigniederlassungen eingerichtet?
- Treten beim Management der Netzwerkgeräte in Ihren Zweigniederlassungen häufig Fehler auf?
- Was tun Sie gegenwärtig, um steigende Datenverkehrsanforderungen zu bewältigen?
- Wie viele IT-Mitarbeiter gibt es in Ihrer Zweigniederlassung?
- Wie viel Zeit und Aufwand benötigen Sie für eine neue Bereitstellung?
- Wie verwalten Sie die Sicherheit Ihrer Zweigniederlassungen?
- Welche Sicherheitsfunktionen haben Sie in Ihren Zweigniederlassungen eingerichtet?
- Was passiert hier am Patchday von Microsoft?

Serie 80 Appliances

Vollständige All-inclusive-Sicherheit für kleinere Zweigstellen

HARDWARE-SPEZIFIKATION FÜR CHECK POINT SERIE-80-APPLIANCES

	Details
10/100/1000-Ports	10
Datenträger- oder Flash-basiert	Flash
Gehäuse	Desktop
Abmessungen (Zoll)	8,75 × 6 × 1,75 Zoll
Abmessungen (metrisch)	220 × 152,5 × 44 mm
Gewicht	1,085 kg
Betriebsumgebung	0 bis 40 °C (5 bis 95 %, nicht kondensierend)
Netzeingang	100–240 VAC, 50/60 Hz, 240 W
Netzteile	12 V / 2 A DC, 24 W
Stromverbrauch (max.)	16,68 W
Compliance	EMV: EN55022+24_2007-ITE FCC: FCCP15B+ICES-003-ITE Sicherheit: UL/c-UL 60950-1_2nd_2007(US+CA) IEC 60950_1_2nd_2005-CB

PERFORMANCE DER CHECK POINT SERIE-80-APPLIANCES

	Details
Firewall-Durchsatz	1.500 Mbits
VPN-Durchsatz	220 Mbits
IPS-Durchsatz	720 Mbits
AV-Durchsatz	100 Mbits
Concurrent Sessions	150.000
VLANs	1.024
Benutzer	Unbegrenzt

SOFTWARE-SPEZIFIKATION FÜR CHECK POINT SERIE-80-APPLIANCES

	Details
Software-Version	R71
Firewall	Ja
IPSec VPN	Ja
IPS	Optional
Anti-Spam and Email Security	Optional
Antivirus and Anti-Malware	Optional
URL Filtering	Optional

UTM-1 Edge N-Serie Appliances

Vollständige All-inclusive-Sicherheit für kleinere Zweigstellen

ÜBERSICHT

Die UTM-1 Edge N-Serie Appliances von Check Point sind komplett ausgestattete, zentral verwaltete Sicherheits-Appliances für Zweigstellen und externe Standorte. Sie basieren auf den gleichen erstklassigen Technologien von Check Point, die von sämtlichen Fortune-100-Unternehmen eingesetzt werden und sind als kabelgebundene sowie als drahtlose Version erhältlich. Die UTM-1 Edge Industrial-Appliances erfüllen die Industrieanforderungen bezüglich Staub, Wärme und Vibrationen und garantieren eine lange Lebensdauer in rauen Umgebungen. Sie enthalten keine beweglichen Teile und bieten flexible Montagemöglichkeiten, darunter DIN-Hutschienen-, Rack- und Wandmontage.

UTM-1 Edge N-Serie

VORTEILE

- Sichert eine gesamte Zweigniederlassung oder kleine Büros mittels einer einzigen, sofort einsetzbaren Appliance
- Firewall-Leistung auf Gigabit-Niveau ab 695 USD
- Schützt das Netzwerk, die Systeme und die Anwender der Zweigniederlassung vor allen Gefahren aus dem Internet – inklusive Spam-E-Mails
- Schnelle und einfache Bereitstellung neuer Geräte
- Große Flexibilität ermöglicht die Verwaltung von bis zu einigen Tausend Systemen an entfernten Standorten über eine zentrale Managementkonsole
- Bietet Langlebigkeit in extremen Industrieumgebungen (UTM-Edge Industrial)

LEISTUNGSMERKMALE

- Umfassender, integrierter, größtmöglicher Sicherheitsschutz, inklusive Schutz der E-Mail-Infrastruktur und mit der bewährtesten Firewall der Branche
- Robuste Netzwerkfunktionen, darunter sichere Hotspots, Hochverfügbarkeitsoptionen, interner Netzwerk-Terminalserver und Quality of Service
- Zentrale Verwaltung im großen Maßstab, die in weniger als 10 Minuten an entfernten Standorten bereitgestellt werden kann und nur ein Minimum an IT-Ressourcen benötigt
- Sichere drahtlose Konnektivität, integrierter Wi-Fi-Access-Point (802.11b/g) mit 802.1x-Unterstützung, IPsec-over-WLAN, RADIUS-, WEP-, WPA- und WPA2-Authentifizierung

GESPRÄCHSEINSTIEG

- Machen Sie sich Sorgen um den gegenwärtigen Zustand der Netzwerksicherheit in Ihren Zweigstellen?
- Wie schützen Sie Ihre Zweigniederlassungen? Welche Sicherheitsmaßnahmen setzen Sie dort gegenwärtig ein?
- Wie viel Zeit und Aufwand kostet die Aufrechterhaltung der Sicherheit Ihrer Zweigniederlassungen gegenwärtig?

INTERESSANT FÜR

- Unternehmen mit mehreren Zweigniederlassungen, die zentral verwaltete, sichere Konnektivität zwischen den Niederlassungen und zum Internet benötigen
- UTM-1 Edge ist auch hervorragend für kleine Unternehmen und Regional-/Zweigniederlassungen mit bis zu 100 Netzwerkteilnehmern geeignet
- Vertikale Schlüsselbranchen: Einzelhandel, Gesundheitswesen, Finanzdienstleistungen und Versicherungen
- Service Provider, die Unternehmen mit mehreren Zweigniederlassungen verwaltete Sicherheitsdienste für Geräte am Firmenstandort anbieten
- Großunternehmen mit vernetzten Systemen in rauen Umgebungen wie Systeme in Produktionshallen und SCADA-Systeme (UTM-Edge Industrial)
- Produktionshallen-/Fabrikations-/Fertigungslinien-Manager (UTM-Edge Industrial)

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Nutzt Technologien, die von sämtlichen Fortune-100-Unternehmen eingesetzt werden
- Enthält zentrales Management, zentrale Richtlinienkontrolle und zentrale Aktualisierung aller Netzwerkkomponenten
- Bietet Streaming-Antivirenlösung für alle Dateigrößen mit minimaler Beeinträchtigung der Leistung

Für UTM-1 Edge Industrial:

- Nutzen Sie geschäftskritische vernetzte Systeme in rauen Umgebungen (Industrial Ethernet-Umgebungen), z. B. in Fertigungslinien?
- Machen Sie sich Sorgen um die gegenwärtige Netzwerksicherheit Ihrer SCADA- und Prozessleitsysteme, Fertigungslinien oder anderer geschäftskritischer Infrastruktursysteme in einer rauen Umgebung?

UTM-1 Edge N-Serie Appliances

Vollständige All-inclusive-Sicherheit für kleinere Zweigstellen

UTM-1 EDGE N SERIES

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Firmwareversion	Embedded NGX 8.X			
Concurrent Users	8/16/32/Unbegrenzt			

HARDWARE-SPEZIFIKATIONEN

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Firewall-Durchsatz (Mbits)	1.000			
VPN-Durchsatz (Mbits)	200			
Gleichzeitige Firewall-Verbindungen	60.000			
LAN-Switch	4 Ports, 10/100/1000 Mbit/s			
WAN-Port	10/100/1000 Mbit/s		ADSL 2/2+	
DMZ/WAN2-Port	10/100/1000 Mbit/s			
USB-Anschlüsse	0	2	2	1
SFP-Port	0		1	0
Steckplatz für ExpressCard 3G-Modem			✔	
Konsolenanschluss (seriell)	✔			
Mobilfunkverbindung	✔			
Wandmontagesatz	✔			

FIREWALL- UND SICHERHEITSFUNKTIONEN

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Patentierte Check Point Stateful Inspection-Firewall	✔			
Application Intelligence (IPS)	✔			
Instant Messenger und P2P-Blockierung/Überwachung	✔			
Port- und Tag-basiertes VLAN	✔			
Netzwerkzugriffskontrolle (802.1x)	✔			
Integrierter RADIUS-Server	✔			
Secure HotSpot (Guest Access)	✔			

ZUSÄTZLICHE DIENSTE*

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Gateway Antivirus	✔			
Unterstützte Antivirus-Protokolle	HTTP, FTP, POP3, IMAP, SMTP, benutzerdefinierte TCP- und UDP-Ports			
On-the-Fly-Komprimierung	✔			
Integriertes Antispam	✔			
Web Filtering	✔			

* Möglicherweise zusätzliche Dienste erforderlich

UTM-1 Edge N-Serie Appliances

Vollständige All-inclusive-Sicherheit für kleinere Zweigstellen

VPN

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Remote Access Client Software	Check Point Endpoint Security, VPN, SecureClient, SecuRemote, L2TP IPsec VPN			
Site-to-Site VPN	✔			
Remote Access VPN	✔			
VPN-Tunnel	400 (mit Verwaltung)			
Remote Access VPN-Profile	Unbegrenzt			
Site-to-Site VPN-Profile	Unbegrenzt			
IPSec-Funktionen	Hardware accelerated DES, 3DES, AES, MD5, SHA-1, Hardware Random Number Generator (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), IPSec compression, IPSec NAT Traversal (NAT-T)			
L2TP VPN-Server	✔			

NETZWERKBETRIEB

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Unterstützte Standards	Statische IP, DHCP, PPPoE, PPTP, Telstra, L2TP			
Backup-ISP und Lastverteilung	✔			
Dialup Backup	Seriell		USB, Seriell	
Traffic Shaper (QoS)	Erweitert*			
Automatisches Gateway-Failover (HA)	✔*			
Dynamisches Routing*	OSPF, BGP, RIP			
Multicast-Routing*	DVMRP, PIM SM v2			
Druckserver	k. A.		✔	

MANAGEMENT

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
HTTP / HTTPS / SSH / SNMP / SMP / SMP On-Demand	✔			
Lokale Diagnose-Tools	Ping, WHOIS, Packet Sniffer, VPN Tunnel Monitor, Connection Table Monitor, Network Monitor, Active Computers Display, Local Logs, Traffic Monitor			

ADSL-MODEM-SPEZIFIKATIONEN

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Unterstützte Standards	ADSL2, ADSL2+, T.1413 G.DMT (G.992.1) G.Lite (G.992.2) ANNEX A (ADSL über POTS), ANNEX B (ADSL über ISDN)			

UTM-1 Edge N-Serie Appliances

Vollständige All-inclusive-Sicherheit für kleinere Zweigstellen

WIRELESS-SPEZIFIKATIONEN**

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Wireless-Protokolle		802.11b (11 Mbit/s) 802.11g (54 Mbit/s) 802.11n (300 Mbit/s) 802.11g (54 Mbit/s)		802.11b (11 Mbit/s) 802.11g (54 Mbit/s) 802.11n (300 Mbit/s)
Wireless Security		VPN over Wireless, WEP, WPA2 (802.11i) WPA-PSK, 802.1x		VPN over Wireless, WEP, WPA2 (802.11i) WPA-PSK, 802.1x
Wireless Distribution System (WDS)		✔*		✔*
Mehrere Access Points		✔*		✔*

TECHNISCHE DATEN

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Abmessungen (H × B × T)	Stromversorgung			
Gewicht	MTBF			
Betriebsumgebung	Temperatur		Betrieb: 0 bis 40 °C Lagerung/Transport: -5 bis 80 °C	
	Luftfeuchtigkeit		10 bis 90 % (nicht kondensierend)	
Stromversorgung	100–240 VAC, 50–60 Hz (länderabhängig)			
MTBF	68.000 Stunden			
Compliance	FCC Teil 15 Klasse B, CE			
Garantie	1 Jahr			

Safe@Office-Appliances

Bewährte Standalone-Lösung für kleine Unternehmen

ÜBERSICHT

Die Safe@Office-Appliances von Check Point sind einfache, preiswerte und zuverlässige Lösungen, um die Sicherheit und die Konnektivität kleiner Unternehmensnetzwerke aufrechtzuerhalten. Dies wird mittels bewährter, integrierter Sicherheits-, Netzwerk- und Konnektivitätsfunktionen erreicht, die ohne weitere Konfiguration sofort zur Verfügung stehen. Speziell für kleine Unternehmen entwickelt schützen die Safe@Office Unified Threat Management-Appliances (UTM-Appliances) Netzwerke mit bis zu 100 Benutzern vor einer Vielzahl von Sicherheitsbedrohungen aus dem Internet, z. B. Viren, Hackerangriffen, Denial-of-Service-Angriffen und Phishing-Versuchen.

VORTEILE

- Erschwingliche und leicht zu verwendende Rundum-Sicherheitslösung für kleine Unternehmen
- Basiert auf bewährten Sicherheitstechnologien, denen sämtliche Fortune-100-Unternehmen vertrauen
- Wurde speziell im Hinblick auf die Einhaltung gesetzlicher Bestimmungen zur Netzwerksicherheit wie HIPPA und PCI entwickelt
- Maximiert durch sicheres Wireless LAN, Webfilterung und VPN-Konnektivität die Produktivität Ihrer Mitarbeiter
- Vereinfacht die kontinuierliche Administration der Sicherheitsrichtlinie
- Gewährleistet die Aufrechterhaltung des Geschäftsbetriebs rund um die Uhr

LEISTUNGSMERKMALE

- Die am besten erprobte und bewährteste Firewall der Branche, die Hunderte Anwendungen und Protokolle absichert
- Zuverlässiges IPsec-VPN für sichere Site-to-Site-Verbindungen und sicheren Fernzugriff
- Integriertes Intrusion Prevention System (IPS), integrierte Streaming-Antivirenlösung und Webfilterfunktionen
- Die Gateway-Antivirenlösung wird kontinuierlich automatisch aktualisiert, um die Sicherheit Ihres Netzwerks aufrechtzuerhalten
- Schnelle Einrichtung und einfache Verwaltung dank vordefinierter Sicherheitsregeln und automatischer Updates
- Integrierte Hochleistungs-Netzwerk- und Konnektivitätsfunktionen
- Modelle mit Wireless LAN, ADSL2/2+ Modem und UMTS-Unterstützung erhältlich

GESPRÄCHSEINSTIEG

- Interessieren Sie sich für eine Netzwerk- und Sicherheitslösung, die speziell auf kleine Unternehmen zugeschnitten wurde und über bewährte Firewall-, VPN-, IPS-, Antiviren- und Webfilterfunktionen verfügt?
- Arbeiten einige Ihrer Mitarbeiter von zu Hause und benötigen sicheren Zugriff auf das Unternehmensnetzwerk?
- Verfügen Sie über mehrere Niederlassungen, die regelmäßig über das Internet kommunizieren und daher eine sichere Verbindung benötigen?
- Müssen Sie branchenspezifische gesetzliche Vorschriften wie PCI DSS oder HIPAA einhalten?

Hinweis: *Safe@Office ist sehr erfolgreich in Branchen, die zur Einhaltung gesetzlicher Vorschriften verpflichtet sind, wie den Payment Card Industry Data Security Standard (PCI DSS) und Health Insurance Portability and Accountability Act (HIPAA).*

INTERESSANT FÜR

- Kleine Unternehmen, die eine umfassende, sofort einsetzbare All-in-One-Sicherheitslösung suchen
- Managed Security Service Provider (MSSP), die ausgelagertes Netzwerk- und Sicherheitsmanagement für kleine Unternehmen anbieten
- Einzelhandelsfilialen, Hotels, Restaurants, Gesundheitseinrichtungen, Versicherungsunternehmen, Kanzleien, Unternehmen aus der Finanz-/Investmentbranche und Kommunalbehörden

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Bietet vertrauenswürdige Sicherheitslösungen, die von sämtlichen Fortune-100-Unternehmen eingesetzt werden
- Blockiert Viren mittels einer auf der Stateful Inspection-Technologie basierenden Streaming-Antivirenlösung am Gateway, bevor diese in Ihr Netzwerk eindringen können
- Enthält alle Perimeter-Sicherheitselemente, die erforderlich sind, um kleine Unternehmensnetzwerke vor multiplen Bedrohungen zu schützen
- Ermöglicht flexibles Sicherheitsmanagement und eine flexible Bereitstellung, so dass die Lösung lokal verwaltet oder vollständig an einen MSSP ausgelagert werden kann
- Die enthaltenen vordefinierten Sicherheitsrichtlinien und regelbasierten, angepassten Richtlinien machen die Serie zu einer idealen Lösung für Unternehmen, die nicht über spezielle IT-Mitarbeiter verfügen
- Vereinfacht mit umfangreichen Netzwerkfunktionen und Konnektivitätsoptionen die Bereitstellung und ermöglicht die Aufrechterhaltung des Geschäftsbetriebs rund um die Uhr
- Freiheit und Kosteneffizienz eines Wireless LAN ohne Gefährdung der Netzwerksicherheit
- Einfache gemeinsame Nutzung von Druckern mit USB-Anschluss durch integrierten Printserver

Safe@Office-Appliances

Bewährte Standalone-Lösung für kleine Unternehmen

SPEZIFIKATIONEN

Safe@Office 1000N	1000N	1000NW	1000N ADSL	1000NW ADSL
Firmwareversion	Embedded NGX 8.2			
Concurrent Users	25/Unbegrenzt			

HARDWARE-SPEZIFIKATIONEN

	1000N	1000NW	1000N ADSL	1000NW ADSL
Firewall-Durchsatz (Mbit/s)	1.000			
VPN-Durchsatz (Mbit/s)	200			
Gleichzeitige Firewall-Verbindungen	60.000			
LAN-Switch	4 Ports, 10/100/1000 Mbit/s			
WAN-Port	10/100/1000 Mbit/s		ADSL 2/2+	
DMZ/WAN2-Port	10/100/1000 Mbit/s			
USB-Ports	0	2	2	1
SFP-Port	0		1	0
Steckplatz für ExpressCard 3G-Modem			✔	
Konsolenanschluss (seriell)	✔			
Mobilfunkverbindung	✔			
Wandmontagesatz	✔			
Abmessungen (B × H × T)	Kabelgebundene Modelle: 200 × 33 × 122 mm (IEG) Wireless-Modelle: 200 × 33 × 130 mm			
Temperatur	-5 bis 80 °C (Lagerung/Transport), 0 bis 40 °C (Betrieb)			
Gewicht	1,45 kg			
Compliance	FCC Teil 15 Klasse B, CE			
Umweltstandards	RoHS, WEEE			
Garantie	Ein Jahr auf die Hardware			

FIREWALL- UND SICHERHEITSFUNKTIONEN

	1000N	1000NW	1000N ADSL	1000NW ADSL
Patentierte Check Point Stateful Inspection-Firewall	✔			
Application Intelligence (IPS)	✔			
Instant Messenger und P2P-Blockierung/Überwachung	✔			
Port- und Tag-based VLAN	✔*			
Network Access Control (802.1x)	✔			
Integrierter RADIUS-Server	✔*			
Secure HotSpot (Guest Access)	✔*			

ZUSÄTZLICHE DIENSTE**

	1000N	1000NW	1000N ADSL	1000NW ADSL
Gateway Antivirus	✔			
Unterstützte Antivirus-Protokolle	HTTP, FTP, NBT, POP3, IMAP, SMTP benutzerdefinierte TCP- und UDP-Ports			
On-the-Fly-Dekomprimierung	✔			
Integriertes Antispam	✔			
Web Filtering	✔			

Safe@Office-Appliances

Bewährte Standalone-Lösung für kleine Unternehmen

VPN

	1000N	1000NW	1000N ADSL	1000NW ADSL
Remote Access Client Software	Check Point VPN-1® SecuRemote™ (enthalten) / L2TP IPSec VPN-Client, Endpoint Connect VPN-Client			
Site-to-Site VPN	✔			
Remote Access VPN	✔			
VPN-Tunnel	400 (mit Verwaltung)			
Remote Access VPN-Profile	5/Unbegrenzt*			
Site-to-Site VPN-Profile	2/Unbegrenzt*			
IPSec-Funktionen	Hardware accelerated DES, 3DES, AES, MD5, SHA-1, Hardware Random Number Generator (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), IPSec Compression, IPSec NAT Traversal (NAT-T)			
L2TP VPN-Server	✔			

NETZWERKBETRIEB

	1000N	1000NW	1000N ADSL	1000NW ADSL
Unterstützte Standards	Statische IP, DHCP, PPPoE, PPTP, Telstra, L2TP			
Backup-ISP und Lastverteilung	✔			
Dialup Backup	Seriell		USB, Seriell	
Traffic Shaper (QoS)	Basic/Advanced*			
Automatisches Gateway-Failover (HA)	✔*			
Dynamisches Routing*	OSPF, BGP, RIP			
Multicast-Routing*	DVMRP, PIM SM v2			
Druckserver	k. A.		✔	

MANAGEMENT

	1000N	1000NW	1000N ADSL	1000NW ADSL
HTTP / HTTPS / SSH / SNMP / SMP / SMP On-Demand	✔			
Lokale Diagnose-Tools	Ping, WHOIS, Packet Sniffer, VPN Tunnel Monitor, Connection Table Monitor, Network Monitor, Active Computers Display, Local Logs, Traffic Monitor			

ADSL-MODEMSPEZIFIKATION

	1000N	1000NW	1000N ADSL	1000NW ADSL
Unterstützte Standards	ADSL2, ADSL2+, T.1413 G.DMT (G.992.1) G.Lite (G.992.2) ANNEX A (ADSL über POTS), ANNEX B (ADSL über ISDN)			

WIRELESS-SPEZIFIKATIONEN***

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Wireless-Protokolle		802.11b (11 Mbit/s) 802.11g (54 Mbit/s) 802.11n (300 Mbit/s) 802.11g (54 Mbit/s)		802.11b (11 Mbit/s) 802.11g (54 Mbit/s) 802.11n (300 Mbit/s)
Wireless Security		VPN over Wireless, WEP, WPA2 (802.11i) WPA-PSK, 802.1x		VPN over Wireless, WEP, WPA2 (802.11i) WPA-PSK, 802.1x
Wireless Distribution System (WDS)		✔*		✔*
Mehrere Access Points		✔*		✔*

* PowerPack-Erweiterung erforderlich
** Zusätzliche Serviceleistung erforderlich
*** Super-G- und XR-Modus nur über bestimmte Wireless-Netzwerkadapter verfügbar. Änderungen bei der tatsächlichen Reichweite in unterschiedlichen Umgebungen vorbehalten

SMB Cloud-Managed Security Services

Managed Security für kleine Unternehmen

ÜBERSICHT

Mit den Check Point SMB Cloud-Managed Security Services erhalten Sie eine kosteneffiziente Komplettlösung. Das Expertenteam von Check Point übernimmt dabei das Management der Sicherheitsfunktionen, sodass sich Ihre Kunden ganz auf ihre geschäftlichen Aktivitäten konzentrieren können.

VORTEILE

- Erstklassige und bewährte Sicherheitslösung mit kontinuierlichem Support durch den Branchenführer
- Einfache Komplettlösung für schnelle Bereitstellung
- Kosteneffiziente Sicherheit ab 19 USD monatlich, wodurch zukünftige Ausgaben für Sicherheitslösungen reduziert werden
- Verständliche Berichte liefern eine gute Übersicht über Bedrohungen und den aktuellen Sicherheitsstatus
- Ausgezeichneter Rund-um-die-Uhr-Support durch Check Point Experten

LEISTUNGSMERKMALE

- Firewall-Schutz
- Dynamisches VPN
- IPS (Intrusion Prevention System)
- Antivirus & Anti-Malware
- URL Filtering
- Anti-Spam & Email Security
- Reporting
- Service-Updates und -Upgrades

INTERESSANT FÜR

- Kunden mit beschränktem IT-Budget
- Unternehmen, die keine oder nur wenige IT-Security Admins haben
- Kleine und mittlere Unternehmen
- Finanzdienstleister, Anwalts- und Steuerkanzleien

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Erstklassige Sicherheit

- Umfassender Netzwerk-, Daten- und Webschutz
- Patentierte Technologie – schützt 98 % der Fortune-500-Unternehmen

Einfach und unkompliziert

- Schnelle Bereitstellung in nur zwei Schritten
- Ausgezeichneter Rund-um-die-Uhr-Support

Attraktive Preise. Transparente Kosten.

- Vollständige Sicherheit schon ab 19 USD im Monat
- All-inclusive-Preise für eine optimale Planung der Betriebsausgaben

GESPRÄCHSEINSTIEG

- Verfügen Sie über ein Budget für die Sicherheit Ihres Unternehmens und wie wird dieses verwaltet?
- Wie schützen und nutzen Sie Ihre Daten?
- Wie gehen Sie mit den wachsenden Sicherheitsbedrohungen um?
- Wie lösen Sie die Sicherheitsherausforderungen bei Mitarbeitern, die extern arbeiten?
- Wie sorgen Sie für Informations- und Netzwerksicherheit innerhalb unterschiedlicher Geschäftsstellen?
- Welchen gesetzlichen Bestimmungen und Sicherheitsrisiken stehen Sie heutzutage gegenüber?

SMB Cloud-Managed Security Services

Managed Security für kleine Unternehmen

SPEZIFIKATIONEN

Leistungsmerkmal	Details
Firewall	• Höchstes Sicherheitslevel durch - Zugangskontrolle - Anwendungssicherheit - Authentifizierung - Network Address Translation (NAT) - Bridge-Modus • Bis zu 1 Gbits Firewall-Durchsatz mit Echtzeit-Traffic-Mix (IMIX) • Patentierte Stateful Packet Inspection (SPI, zustandsorientierte Paketüberprüfung)
Firewall	• Vereinfachtes Site-to-Site VPN • Erweiterte IPsec VPN-Sicherheit • Flexible Unterstützung durch Remotezugriff • Verschiedene VPN-Konnektivitätsmodi für Remotezugriff
IPS (Intrusion Prevention System) Premium	• Hochleistungs-IPS-Durchsatz • Erhöhte Effizienz durch dynamisches Threat-Management • Präventive Sicherheitsupdates zum Schutz vor neuen Bedrohungen • Erstklassiger Schutz vor Sicherheitslücken bei Microsoft und Adobe Reader
Antivirus Premium	• Viren- und Malware-Scans in Echtzeit • Kontinuierliche Echtzeit-Scans von heruntergeladenen Dateien • Scanning komprimierter Dateien • Zentrale, granulare Konfiguration und Durchsetzung von Richtlinien
Anti-Spam Premium	• Anti-Spam auf Basis der Reputation der IP-Adresse des Absenders • Inhaltsbasiertes Anti-Spam anhand musterbasierter Erkennung • Granulare Kontrolle mit Black/ White-Listen • Virus- und Malwareschutz durch Scans von E-Mail-Inhalten und -Anhängen • Zero-Hour-Schutz gegen Spam und Malware Schutz der E-Mail-Infrastruktur vor Bedrohungen wie Denial of Service Angriffen
URL Filtering Premium	• Anpassbare Benachrichtigung oder Umleitungsseiten • Abdeckung von über 25 Millionen URLs • Über 40 vorkonfigurierte Content-Kategorien • Kontrollfunktion durch Blacklists/Whitelists • Kontinuierliche Aktualisierung durch den Check Point Update Service

DDoS Protector Appliances

Spezialisierter Schutz vor bekannten und unbekannten DDoS-Angriffen

ÜBERSICHT

Die Check Point DDoS Protector™-Appliances schützen innerhalb von Sekunden vor DoS-Angriffe (Denial of Service-Attacken) bei einem Durchsatz von bis zu 12 Gbits. Hacker setzen modernste Techniken ein, um Unternehmensbereiche zu identifizieren, die von traditionellen Sicherheitslösungen nicht geschützt werden. Diese Angriffe können zu Netzwerkausfällen in Unternehmensbereichen führen, die von der Verfügbarkeit des Netzwerks abhängig sind. Die DDoS Protectors erweitern die Sicherheitsperimeter zum Schutz vor DDoS-Angriffen, noch bevor diese Schaden anrichten können.

VORTEILE

- Schutz vor neuen DDoS-Angriffen, um Auswirkungen auf den Betrieb zu minimieren
- Modernste Technologien sorgen für die Aufrechterhaltung von Webdiensten während eines Angriffs
- Sofort einsetzbare Appliance
- Integrierte Check Point-Lösungen zum Sicherheitsmanagement für größere Transparenz und Kontrolle
- Leistungsstarke DDoS-Lösungen mit 14 Gbits Kapazität und 12 Bits Durchsatz
- Mehrschichtiger Schutz vor verschiedenen Angriffsarten
- Individuell angepasster Schutz für unterschiedliche Unternehmensgrößen und Sicherheitsanforderungen
- Flexible Bereitstellungsoptionen, inklusive Vor-Ort-Installation oder Bereitstellung durch den ISP

LEISTUNGSMERKMALE

- Schutz vor jeglicher Art von DDoS-Angriffen
- Sicherer Schutz vor Angriffen auf Netzwerke und Anwendungen
- Flexible Filtermodule zur aktiven Erkennung und Abwehr von schädlichen Exploits
- Schutz vor HTTP-Angriffen
- Schutz vor Angriffen durch Bandbreitenüberflutung
- Schnelle, individuelle Signaturerstellung zur Verhinderung von Geschäftsausfällen

INTERESSANT FÜR

- Jede Art von E-Commerce-Anbietern
- Internetdienstanbieter, Netzbetreiber
- Finanzdienstleister, Behördenkunden, Militärstellen, Verkehrs- und Energieinfrastruktur-Anbieter

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- 7 dedizierte Hochleistungappliances
- Multi-Layer-Schutz
- Schnelle Reaktion bei Angriffen
- Individueller Schutz für jedes Unternehmen
- Integriertes Sicherheitsmanagement

GESPRÄCHSEINSTIEG

- Welche Bedenken haben Sie bezüglich zunehmender DDoS-Angriffe?
- Welche Art von DoS-Schutz verwenden Sie derzeit?
- Welche Probleme hatten Sie bisher mit Ihrer aktuellen DDoS-Lösung?
- Welches ist der erste Angriffspunkt in Ihrem Netzwerk?
- Welchen Schutz haben Sie gegen aktuelle Angriffe auf Anwendungsebene installiert?

DDoS Protector Appliances

Spezialisierter Schutz vor bekannten und unbekannten DDoS-Angriffen

PERFORMANCE- UND HARDWARE-SPEZIFIKATIONEN

DDoS Protector-Appliance	506	1006	2006	3006	4412	8412	12412
Netzwerkgröße	Unternehmen				Rechenzentrum		
Kapazität[1]	500 Mbits	1 Gbits	2 Gbits	3 Gbits	4 Gbits	8 Gbits	14 Gbits
Durchsatz[2]	500 Mbits	1 Gbits	2 Gbits	3 Gbits	4 Gbits	8 Gbits	12 Gbits
Max. Concurrent Sessions	2.000.000				4.000.000		
Max. Vorbeugungsrate gegen DDoS-Flutangriffe	1.000.000 Pakete/Sekunde				10.000.000 Pakete/Sekunde		
Latenz	<60 Mikrosekunden						
Echtzeit-Signaturen	Erkennen und Schützen in weniger als 18 Sekunden						
Inspektionsports	(4) 10/100/1000-Kupfer-Ethernet (2) Gigabit-Ethernet (SFP)				(8) 10/100/1000-Kupfer-Ethernet (4) Gigabit-Ethernet (SFP) (4) 10-Gigabit-Ethernet (XFP)		
Managementports	(2) 10/100/1000-Kupfer-Ethernet (1) RS-232						
Netzwerkbetrieb	Transparente L2-Weiterleitung						
Bereitstellungsmodus	In-line; SPAN Port Monitoring; Copy Port Monitoring; Local Out-of-Path; Out-of-Path Mitigation (Scrubbing Center Solution)						
Unterstützung für Tunneling-Protokolle	VLAN Tagging, L2TP, MPLS, GRE, GTP						
IPv6	Unterstützung für IPv6-Netzwerke / Blockieren von IPv6-Angriffen						
Richtlinienaktion	Blockieren & melden, nur melden						
Blockieraktionen	Paket verwerfen, zurücksetzen (Quelle, Ziel, beide), anhalten (Quelle, Quellport, Ziel, Zielport oder jede Kombination), Anfrage/Antwort für HTTP- und DNS-Angriffe						
Hochverfügbarkeit (Fail-open/Fail-close)	Internes Fail-open/Fail-close für Kupfer-Ports, internes Fail-close für SFP-Ports, optionales Fail-open für SFP-Ports[3]				Internes Fail-open/Fail-close für Kupfer-Ports, internes Fail-close für SFP- und XFP-Ports, optionales Fail-open für SFP- und XFP-Ports[4]		
Duale Stromversorgung	Optional				Ja – im laufenden Betrieb austauschbar		
Erweiterter interner Overload-Mechanismus	Ja						
Aktiv-Passiv-Cluster	Ja						
Abmessungen (B × T × H)	424 × 457 × 44 mm				424 × 600 × 88 mm		
Gewicht	7,2 kg (Dual-PS-Option 8,7 kg)				18,0 kg		
Automatisch umschaltbare Netzteile	100–120 V / 200–240 VAC, 47–63 Hz oder 38–72 VDC						
Stromverbrauch	177 W (Dual-PS-Option 147 W)				476 W		
Wärmeableitung	604 BTU/h (Dual-PS-Option 501 BTU/h)				1.623 BTU/h		
Betriebstemperatur	0–40 °C						
Luftfeuchtigkeit (nicht kondensierend)	5 bis 95 %						
Sicherheitszertifizierungen	EN 60950-1:2006, CB – IEC 60950-1, cTUVus				EN, UL, CSA, IEC #60950-1		
EMV	EN 55022, EN 55024, FCC Part 15B Klasse A						
Andere Zertifizierungen	CE, FCC, VCCI, CB, TUV, UL/cUL, CCC, C-Tick, RoHS						

[1] Die Kapazität wird als maximaler Datenverkehr gemessen, wenn keine Sicherheitsprofile konfiguriert sind.
[2] Der Durchsatz wird mit verhaltensorientiertem IPS-Schutz und Signatur-IPS anhand eines eCommerce-Schutzprofils gemessen.
[3] Externer Fail-open-Glasfaserswitch mit SFP-Ports ist gegen Aufpreis erhältlich.
[4] Externer Fail-open-Glasfaserswitches mit SFP- oder XFP-Ports sind gegen Aufpreis erhältlich.

Zubehör für Check Point-Appliances 2012

Übersicht über sämtliches 2012 Appliance-Zubehör

ÜBERSICHT

Check Point-Appliances weisen flexible Erweiterungsmöglichkeiten auf, mit denen sie den unterschiedlichen Anforderungen moderner Unternehmensnetzwerke gerecht werden. Das modulare Design und die große Auswahl an verfügbaren Netzwerkoptionen für die Appliances der 4000-, 12000 und 21000-Serie ermöglichen diesen Gateways nicht nur eine Vielzahl an Verbindungsoptionen, sondern gestatten auch die Anpassung an jede Art von Netzwerktopologie.

Das höchste Ziel von Check Point ist es, für verfügbare Netzwerke und unterbrechungsfreie Geschäftsabläufe zu sorgen. Die 4800 (nur mit redundanter Stromversorgung), 12000 und 21400 Appliances bieten Funktionen wie redundante und Hot-Swap-fähige Speicher und Netzteile. Kombiniert sorgen diese Funktionen für eine optimierte Systemverfügbarkeit und eine verbesserte Geschäftskontinuität. Mithilfe der Montageschienen, die mittlerweile Standard bei vielen Gateway-Appliances sind, wird eine schnelle und einfache Rackmontage ermöglicht und die Wartbarkeit des Systems verbessert.

NETZWERK

Die 4000 und 12000 Appliances können mit unterschiedlichen Netzwerk-Schnittstellenkarten wie 1-GbE-Kupfer, 1-GbE-Glasfaser oder 10-GbE-Glasfaser bestellt werden. Je nach Appliance und der Anzahl an verfügbaren Erweiterungssteckplätzen variiert die Portdichte. Die Netzwerk-Schnittstellenkarten können dank der 10-GbE-Schnittstellenoptionen, die ab dem 4800er Modell verfügbar sind, zwischen den 4000 und 12000 Appliances ausgetauscht werden.

Die 21400 Appliances können mit Netzwerk-Schnittstellenkarten für 1-GbE-Kupfer, 1-GbE-Glasfaser oder 10-GbE-Glasfaser bestellt werden. Die Portdichte kann auf 37 1-GbE-Kupferanschlüsse oder 36 1-GbE-Glasfaseranschlüsse erhöht werden. Für die 21400 Appliance ist zusätzlich eine 4-Port 10-GbE-Glasfaseroption erhältlich, mit der sich die maximale Netzwerkkapazität auf 12 x 10-GbE-Port erhöhen lässt.

VORTEILE

- Dank anpassbarer Netzwerkschnittstelle in jeder Netzwerkumgebung einsetzbar
- Erweiterung der Appliances um mehr Netzwerkkapazität und Sicherheitsfunktionen, um dem wachsenden Bedarf des Unternehmens gerecht zu werden
- Gesteigerte Geschäftskontinuität durch redundante und Hot-Swap-fähige Speicher und Netzteile
- Vereinfachte Wartung durch Nutzung der „Slide Rails“

LEISTUNGSMERKMALE

- Flexible Netzwerkerweiterungsoptionen
  - 10/100/1000Base-T
  - 1000Base-F SPF
  - 10GBase-F SPF+
- Redundante Festplatte mit RAID-1-Support
- Redundante, Hot-Swap-fähige Stromversorgung
- Montageschienen

KAPAZITÄT DER NETZWERKANSCHLÜSSE (4000, 12000 UND 21400 APPLIANCES)

	4200	4400	4600	4800	12200	12400	12600	2100	21400
10/100/1000Base-T/ 100/1000Base-T (Standard/max. Ports)	4/8	8/12	8/16	8/16	10/26	14/26	13/26	14/26	13/37
1000Base-F SFP (Standard/max. Ports)	0/4	0/4	0/4	0/4	0/4	0/12	0/12	0/12	0/36
10GBase-F SFP+ (Standard/max. Ports)	k. A.	k. A.	k. A.	0/2	0/4	0/12	0/12	0/12	0/12
Erweiterungssteck-plätze	1	1	1	1	1	1	3	3	3

Zubehör für Check Point-Appliances 2012

Übersicht über sämtliches 2012 Appliance-Zubehör

NETZWERK-E/A-MODULE (4000 UND 12000 APPLIANCES)

SKU	CPAC-4-1C	CPAC-4-1F	CPAC-8-1C	CPAC-2-10F	CPAC-4-10F
Unterstützte Appliances	4200, 4400, 4600, 4800, 12200, 12400, 12600	4200, 4400, 4600, 4800, 12200, 12400, 12600	4800, 12200, 12400, 12600	4800, 12200, 12400, 12600	12200, 12400, 12600
Anzahl der Ports	RJ-45 (Kupfer) 10/100/1000Base-T	SFP	RJ45 (Kupfer) 10/100/1000Base-T	SFP+	SFP+
Geschwindigkeit	1 Gbit/s	1 Gbit/s	1 Gbit/s	10 Gbit/s	10 Gbit/s
Mögliche Transceiver	k. A.	CPAC-TR-1SX CPAC-TR-1LX	k. A.	CPAC-TR-10SR CPAC-TR-10LR	CPAC-TR-10SR CPAC-TR-10LR

NETZWERK-TRANSCEIVER*-SPEZIFIKATION (4000 UND 12000 APPLIANCES)

SKU	CPAC-TR-1SX	CPAC-TR-1LX	CPAC-TR-10SR	CPAC-TR-10LR
Formfaktor	SFP	SFP	SFP+	SFP+
Protokoll	1,25 Gbit/s 1000Base-SX Ethernet	1,25 Gbit/s 1000Base-LX Ethernet	10GBASE-SR 10G Ethernet	10GBASE-LR 10G Ethernet
Wellenlänge (nm)	850	1.310	850	1.310
Konnektor	LC	LC	LC	LC
Entfernung (max.)	1 Gbit/s	1 Gbit/s	1 Gbit/s	10 Gbit/s
Unterstützter Kabeltyp	Orange: Multimode 50/125 µm MMF (OM3)	Gelb: Singlemode 5 km bei 9 µm	Orange: Multimode 50/125 µm Glasfaser (OM3)	Gelb: Singlemode 10 km bei 9 µm
Eingangspegel (Eingangsleistung) dBm	-18 dBm	-19 dBm	-17 dBm	-19 dBm
Ausgangspegel (Übertragungsleistung) dBm	-2,5 bis -9 dBm	-3 bis -9,5 dBm	-1 bis -9,5 dBm	-3 bis -11 dBm

NETZWERK-E/A-MODULE (21400 APPLIANCES)

SKU	CPAC-12-1C-21000	CPAC-12-1F-21000	CPAC-4-10F-21000
Anzahl der Ports:	12	12	4
Anschlusstyp:	RJ-45 (Kupfer) 10/100/1000Base-T	SFP 1000Base-T\SX\LX	SFP+ 10GBase-SR\LR
Geschwindigkeit	1 Gbit/s	1 Gbit/s	10 Gbit/s
Mögliche Transceiver	k. A.	CPAC-TR-1SX-21000 CPAC-TR-1LX-21000 CPAC-TR-1T-21000	CPAC-TR-10SR-21000 CPAC-TR-10LR-21000

Zubehör für Check Point-Appliances 2012

Übersicht über sämtliches 2012 Appliance-Zubehör

NETZWERK-TRANSCEIVER*-SPEZIFIKATION (21400 APPLIANCES)

SKU	CPAC-TR-1T-21000	CPAC-TR-1SX-21000	CPAC-TR-1LX-21000	CPAC-TR-10SR-21000	CPAC-TR-10LR-21000
Formfaktor	SFP	SFP	SFP	SFP+	SFP+
Protokoll	1000Base-T kompatibel	1,25 Gbit/s 1000Base-SX Ethernet	1,25 Gbit/s 1000Base-LX Ethernet	10GBASE-SR 10G Ethernet	10GBASE-LR 10G Ethernet
Wellenlänge (nm)		850	1.310	850	1.310
Konnektor	RJ-45	LC	LC	LC	LC
Entfernung (max.)	100 m	500 m bei 50/125 µm MMF	5 km	300 m	10 km
Unterstützter Kabeltyp	Cat 5	Orange: Multimode 50/125 µm MMF (OM3)	Gelb: Singlemode 5 km bei 9 µm	Orange: Multimode 50/125 µm Glasfaser	10GBASE-LR 10G Ethernet
Eingangspegel (Eingangsleistung) dBm	k. A.	-18 dBm	-19 dBm	-17 dBm	-19 dBm
Ausgangspegel (Übertragungsleistung) dBm	k. A.	-2,5 bis -9 dBm	-3 bis -9,5 dBm	-1 bis -9,5 dBm	-3 bis -11 dBm

* Nur über Check Point angebotene Transceivers werden unterstützt.

SECURITY ACCELERATION-MODUL (21400 APPLIANCE)

SKU	CPAC-SAM108
Anzahl der Security-Kerne	108
Kartentyp	Acceleration-Modul für 21000 Appliances
	Performance-Upgrade (bis 21400)
Firewall	110 Gbit/s
Paket pro Sekunde	60.000.000
Sitzung pro Sekunde	300.000
Firewall-Latenzzeit	Unter 5 µs

FESTPLATTENSPEICHER

Redundante Laufwerke unterstützen RAID-1-Spiegelung, wodurch die Ausfallsicherheit erhöht wird. Eine RAID-Statusüberwachung ist über SNMP verfügbar.

REDUNDANTE SPEICHEROPTIONEN (4000, 12000 UND 21400 APPLIANCES)

	4200	4400	4600	4800	12200	12400	12600	21400
Standard (GB)	1 x 250	1 x 250	1 x 250	1 x 250	1 x 500	1 x 500	2 x 500	2 x 500
Redundante Festplatte (GB)	n. v.	n. v.	n. v.	n. v.	1 x 500 (optional)	1 x 500 (optional)	Enthalten	Enthalten
Maximum	1 x 250	1 x 250	1 x 250	1 x 250	2 x 500 RAID 1	2 x 500 RAID 1	2 x 500 RAID 1	2 x 500 RAID 1

SPEZIFIKATION DER FESTPLATTENSPEICHER (12200, 12400, 12600, 21400 APPLIANCES)

	12200	12400 und 12600	21400
SKU	CPAC-HDD-500G-12200	CPAC-HDD-500G	CPAC-HDD-500G-21000
Kapazität	500 GB	500 GB	500 GB
Schnittstelle	SATA, 3 Gbit/s	SATA, 3 Gbit/s	SATA, 3 Gbit/s
RPM	7.200	7.200	7.200
Cache	32 MB	64 MB	64 MB

Zubehör für Check Point-Appliances 2012

Übersicht über sämtliches 2012 Appliance-Zubehör

STROMVERSORGUNG

Die doppelte Stromversorgung erhöht die Gesamtzuverlässigkeit der Appliance. Fällt ein Netzteil aus, wird man über ein akustisches Signal alarmiert. Der Status der Stromversorgung wird zusätzlich über SNMP oder im WebUI-Status überwacht.

STROMVERSORGUNGSOPTIONEN (4000, 12000, 2140 APPLIANCES)

	4200	4400	4600	4800	12200	12400	12600	21400
Redundante Stromversorgung (1+1)	n. v.	n. v.	n. v.	Optional	Optional	Enthalten	Enthalten	Enthalten

SPEZIFIKATION DER STROMVERSORGUNG (4800, 12200, 12400, 12600, 21400 APPLIANCES)

	4200	4400	4600	4800	12200
SKU	CPAC-PSU-4800	CPAC-PSU-12200	CPAC-PSU-12400	CPAC-PSU-12600	CPAC-PSU-21000
Eingangsspannung	110–240 VAC	110–240 VAC	110–240 VAC	110–240 VAC	110–240 VAC
Eingangsstrom	3–1,5 A	3–1,5 A	3–1,5 A	3–1,5 A	3–1,5 A
Frequenz	47–63 Hz	47–63 Hz	47–63 Hz	47–63 Hz	47–63 Hz
Thermische Leistung	425,6 BTU	412,9 BTU	450,4 BTU	750,6 BTU	1.533 BTU
Ausgangsleistung	275 W	275 W	300 W	400 W	910 W

SPEICHER

Zusätzlicher Systemspeicher erhöht die Verbindungskapazität der Appliance und verbessert die Gesamtleistung beim Aktivieren zusätzlicher Software-Blades.

SPEICHERERWEITERUNGSOPTIONEN

	4200	4400	4600	4800	12200	12400	12600	21400
Standard (GB)	4	4	4	4	4	4	6	12
Optionale Speichererweiterung (GB)	n. v.	n. v.	n. v.	4	4,8	4,8	6	12
Maximum (GB)	4	4	4	8	12	12	12	24

SPEICHERSPEZIFIKATION (4800, 12200, 12400, 12600, 21400 APPLIANCES)

	4200	4400	4600	4800	12200
SKU	CPAC-RAM4GB	CPAC-RAM4GB	CPAC-RAM4GB-12400	CPAC-RAM6GB-12600	CPAC-RAM12GB-21000
Kapazität	4 GB	4 GB	4 GB	6 GB	12 GB
Typ	DDR3	DDR3	DDR3	DDR3	DDR3
Anzahl der Module	1 x 4 GB	1, 2 x 4 GB	1, 2 x 4 GB	6 x 1 GB	6 x 2 GB
ECC	Nein	Nein	Nein	Ja	Ja

MONTAGESCHIENEN

Die Montageschienen sind einfach anzubringen (5-10 Minuten) und bieten einen optimalen Wartungszugriff für 4000, 12000 und 21400 Appliances in einem Standard-Rack (48,26 cm) (siehe Spezifikation EIA-310-D).

OPTIONEN FÜR MONTAGESCHIENEN

	4200	4400	4600	4800	12200	12400	12600	21400
Montageschiene	optional	optional	optional	Enthalten	Enthalten	Enthalten	Enthalten	Enthalten

MONTAGESCHIENEN-SPEZIFIKATION (4000 APPLIANCES)

- SKU: CPAC-RAILS
- Mindesttiefe: 66 cm (25,9 Zoll)
- Maximale Tiefe: 80 cm (31,5 Zoll)

MONTAGESCHIENEN-SPEZIFIKATION (21400 APPLIANCES)

- Mindesttiefe: 66 cm (26 Zoll)
- Maximale Tiefe: 88,9 cm (35 Zoll)

Virtual Systems

Virtualisierung von Security Services unter GAiA

ÜBERSICHT

Die Check Point Virtual Systems ermöglicht eine Konsolidierung von hunderten von Security-Systemen auf einer einzigen Hardware-Plattform und damit umfassende Kosteneinsparungen sowie eine Konsolidierung der Infrastruktur. Auf eine Appliance konsolidiert, stellt VS herausragende Firewall-, VPN-, URL Filtering- und Intrusion-Prevention-Technologien für eine Vielzahl von Netzwerken zur Verfügung und sorgt für deren sichere Verbindung untereinander und zu gemeinsam genutzten Ressourcen, wie dem Internet und DMZs. Funktionserweiterungen sind jederzeit über den Erwerb zusätzlicher Software Blades möglich. Alle Security-Systeme, ob virtuell oder real, werden über das Check Point SmartCenter™ oder Multi-Domain Security-Management-Konsolen zentral verwaltet.

Durch den Betrieb eines virtuellen Netzwerks mit hunderten von Routern, Switches und Gateways ermöglicht VS jedem Unternehmen die Optimierung von Platzbedarf und Kosten. Eine ideale Plattform ist VS auch für MSPs (Managed Service Provider) mit Chancen auf neuen Subskriptionsumsatz, da neue Security-Services sehr schnell und einfach bereitgestellt werden können. Dazu gehören virtualisiertes Value Added Content-Filtering, VPN, Netzwerksegmentierung und Firewall-Services, die mit Hilfe des Virtual Systems Wizard sofort und zu geringen Kosten vorgehalten werden können.

VORTEILE

- Konsolidierung bis hin zu 250 von Security Gateways auf einer einzigen Appliance, verbesserte Hardware-Ausnutzung und Reduktion von Energie-, Platz- und Kühlungsbedarf
- Lineare Skalierbarkeit, Load-Sharing und Multi-Gigabit-Performance
- Flexible Einsatzoptionen, einschließlich offener Plattformen und einer vollständigen Reihe schlüsselfertiger Appliances
- Zentralisiertes Security-Management vereinheitlicht das physische und virtuelle Management in einer einzigen Lösung

LEISTUNGSMERKMALE

- Unterstützung der Check Point Software-Blade-Architektur (Ausnahme: DLP, Anti-Spam)
- GAiA 64-Bit-Betriebssystem
- Unterstützung von Check Point Appliances und Open Servern (siehe HCL)
- Flexible virtuelle Konnektivität mit Unterstützung einer Vielzahl von Routing-Szenarien
- Hochleistungssicherheitsfunktionen sorgen für kontinuierlich maximale Leistung der offenen Server und Appliances
- Umfassende Sicherheitsdienste stellen sichere Verbindungen zwischen mehreren Netzwerken oder VLAN und gemeinsam genutzten Ressourcen innerhalb komplexer Infrastrukturen her
- Erprobte und ausgereifte Sicherheitsmanagementarchitektur bietet leistungsfähige Werkzeuge für die zentrale Konfiguration, Verwaltung und Überwachung

INTERESSANT FÜR

- Managed Security Service Provider (Anbieter verwalteter Sicherheit, z. B. MSSP, ASP) sowie große Unternehmen und Organisationen, die ihre Rechenzentren oder großen Standortnetzwerke mittels VLAN-Segmentierung modernisieren, neu konfigurieren oder erweitern möchten
- Regierungsbehörden, Gesundheitseinrichtungen und Produktionseinrichtungen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Bietet einfache Verwaltung und Bereitstellung mit feingranularen Kontrollfunktionen für MSSP-Endkunden oder Enterprise-Domänen
- Stellt dank Schutz-Updates über SmartDefense Services die tiefgehendste und modernste virtualisierte Sicherheit bereit
- Optimiert die Implementierung und Konfiguration der virtuellen Systeme mit Assistenten und Vorlagen
- Sichert unterschiedlichste VoIP-Netzwerke
- Unterstützt verschiedene Optionen für den sicheren Client-Fernzugriff

GESPRÄCHSEINSTIEG

- Welche Elemente Ihres Netzwerks wurden virtualisiert?
- Bestehen bereits Pläne für eine Virtualisierung?
- Wie viele Regeln enthält die Regelbasis Ihrer Check Point-Firewalls?
- Haben Sie in Erwägung gezogen, diese Regelbasen aufzuteilen und sie mittels mehrerer Gateways auf verschiedene Arten von
- Perimeter-Datenverkehr anzuwenden?

Virtual Systems

Virtualisierung von Security Services unter GAiA

SPEZIFIKATIONEN

Betriebssystem	GAiA (R75.40VS) oder später
Unterstützte Gateways	Check Point Appliances und Open Servers
Mindestspeicheranforderungen	2 GB
Unterstützte Technologien	ClusterXL, CoreXL, SSL inspection
Monitoring	Überwachung von Ressourcen (CPU & Speicher), pro virtuellem System via SNMP

SPEZIFIKATIONEN

Appliance Speicher	Appliance Speicher (GB, Standard / max.)	Maximal unterstützte virtuelle Systeme (Standard / max. Speicher)
2200	2 / 2 GB	3 / 3
4200	4 / 4 GB	3 / 3
4400	4 / 4 GB	10 / 10
4600	4 / 4 GB	10 / 10
4800	4 / 8 GB	20 / 25
12200	4 / 12 GB	20 / 50
12400	4 / 12 GB	25 / 75
12600	6 / 12 GB	75 / 150
21400	12 / 24 GB	125 / 250
UTM-1 3070	4 / 4 GB	10 / 10
Power-1 9070	4 / 4 GB	50 / 50
Power-1 11000	6 / 6 GB	75 / 75
IP 1280	4 / 8 GB	10 / 50
IP 2450	4 / 8 GB	50 / 75

VIRTUAL SYSTEM APPLIANCES

Die Modellreihen: 4400, 4600, 4800 und 12200 stehen außerdem als vorkonfiguriertes Virtual System Appliances zur Verfügung. (Einzelgerät oder HA/VSLS). Siehe hierzu auch: http://www.checkpoint.com/products/virtual-systems/index.html“

Security Gateway Virtual Edition

Virtualisierung von Security Services unter VMware ESX/ESXi

ÜBERSICHT

Check Point VPN-1 VE™ (Virtual Edition) schützt virtuelle Umgebungen vor internen und externen Bedrohungen. VPN-1 VE basiert auf der gleichen erstklassigen Sicherheitstechnologie von Check Point, die auch in den Produkten für physische Netzwerksicherheit zum Einsatz kommt. Die Lösung kombiniert Firewall, VPN und Intrusion Prevention System (IPS), um virtuelle Maschinen (VMs), virtuelle Anwendungen und virtuellen Datenverkehr zu schützen. VPN-1 VE ist die einzige Lösung für komplette Sicherheit, die den Datenverkehr zwischen VMs untersucht und dadurch sowohl vor internen als auch vor externen Bedrohungen schützt. Sie wird über eine einzige Oberfläche verwaltet, um konsistentes und effizientes Sicherheitsmanagement zu gewährleisten.

VORTEILE

- Schützt virtuelle Systeme mit erstklassigen Sicherheitsfunktionen
- Bietet umfassende und erweiterbare Sicherheit zum Schutz von VMware-Umgebungen
- Schützt mit Hilfe des Check Point Update Service vor neu aufkommenden Bedrohungen
- Ermöglicht das einheitliche Management physischer und virtueller Umgebungen

LEISTUNGSMERKMALE

- Bewährte Firewall kann ohne weitere Konfiguration hunderte Anwendungen, Protokolle und Dienste überprüfen
- Integrierte IPS-Funktion nutzt signaturbasierte und auf Protokoll-Anomalien basierende Erkennung von Eindringlingen, um geschäftskritische Dienste vor bekannten und unbekannten Angriffen zu schützen
- Zentrales, einheitliches Management stellt konsistente Sicherheit auf allen Gateways sicher und minimiert die Ausgaben für getrennte Managementkonsolen
- Höchste Leistung, Verfügbarkeit und Lastverteilung
- Vorkonfiguriert für schnelle Bereitstellung und dennoch anpassbar für den Schutz spezieller Umgebungen
- Integrierte Firewall, VPN- und IPS-Funktion sowie Verfügbarkeit mit umfassenden XTM-Fähigkeiten vereinfacht die Bereitstellung und die Administration
- Erzwungene Sicherheit für VMotion, um virtuelle Maschinen, die sich gerade im Betrieb befinden, während der Live-Migration zu schützen
- VMware-Zertifizierung für VMware ESX

INTERESSANT FÜR

- Unternehmen jeder Größe (kleine bis mittelgroße Unternehmen, große Unternehmen) und Service Provider
- Finanzdienstleister/Bankinstitute, Gesundheitseinrichtungen, Produktionseinrichtungen, Behörden/Militäreinrichtungen, Kommunikationsunternehmen, Versorgungseinrichtungen und ISP/MSP

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Schützt virtuelle Maschinen mittels bewährter Anwendungskontrolle und Angriffsschutz vor internen und externen Bedrohungen
- Bietet konsistente Sicherheit für virtuelle und physische Umgebungen
- Einheitliches Management – VPN-1 VE wird über das gewohnte Check Point Security Management verwaltet. Kunden müssen daher keine neuen Managementsysteme erwerben.
- Bietet vollständige Firewall-, VPN- und IPS-Funktionalität und kann mit oder ohne vollständige XTM-Fähigkeiten bereitgestellt werden
- Garantierte Interoperabilität mit VMware ESX

GESPRÄCHSEINSTIEG

- Wie schützen Sie Ihre virtuellen Appliances und den virtuellen Netzwerkverkehr vor internen und externen Bedrohungen?
- Machen Sie sich Sorgen über die Aufrechterhaltung der Sicherheit, wenn in Betrieb befindliche VMs mittels VMotion migriert werden?
- Haben Sie die Möglichkeit, Einblick in den Datenverkehr zwischen den VMs bzw. virtuellen Anwendungen in Ihren ESX-Serverumgebungen zu nehmen?
- Sind Sie daran interessiert, Ressourcen für entfernte Büros und Zweigstellen schnell und effizient bereitzustellen?

Security Gateway Virtual Edition

Virtualisierung von Security Services unter VMware ESX/ESXi

SPEZIFIKATIONEN

Funktion	Beschreibung
Unterstützte VMware-Server	• VMware vSphere • ESX v4.0 • ESX v4.1 • ESXi v4.0 • ESXi v4.1 • ESX v5.0 - Network Mode
Unterstützte Check Point-Lösungen	• Security Gateway Software Blades R75.20
Mindestanforderungen für die Virtuelle Appliance	• Zugewiesener Arbeitsspeicher: 512 MB • Festplattenspeicher: 12 GB

SPEZIFIKATIONEN

Funktionen und Software Blades	Hypervisor Mode	Network Mode
Firewall	Ja	Ja
IPsec VPN	Nein	Ja
IPS	Ja	Ja
URL Filtering	Teilweise (siehe SK 00786175)	Ja
Email Security und Anti-Spam	Nein	Ja
Application Control	Teilweise (siehe SK 00785612)	Ja
DLP	Teilweise (siehe SK 00785488)	Ja
Anti-Malware	Teilweise (siehe SK 00525807)	Ja
Identity Awareness	Teilweise (siehe SK 00784665)	Ja
Web Security	Ja	Ja
VoIP	Nein	Ja
QoS	Nein	Ja
Dynamic Routing	Nein	Ja
NAT	Nein	Ja
CoreXL	Nein	Ja

Virtual Appliance für Amazon Web Services

Sicherheit für virtuelle Umgebungen in der Amazon Cloud

ÜBERSICHT

Mit der Check Point Virtual Appliance für Amazon Web Services können Kunden ihre Sicherheitslösung auf die Cloud erweitern und dabei alle Sicherheitsfunktionen der Check Point Software Blades nutzen. Diese einfach bereitzustellende, virtuelle Appliance – ein Sicherheits-Gateway für virtuelle Umgebungen in der Amazon Cloud – verhindert Netzwerkangriffe und Datenverluste und sorgt für sichere Verbindungen in dynamischen Cloud-Computing-Umgebungen.

VORTEILE

Bereitstellung von Check Point Software Blades für Sicherheit in der Amazon Cloud

- Firewall und IPS Software Blades schützen Ressourcen in der Cloud vor Angriffen
- VPN und Mobile Access Software Blades sorgen für sichere Verbindungen und Mobilität
- Das DLP Software Blade schützt Daten in der Cloud und verhindert Datenverluste

Schnelle Einrichtung erweiterter Sicherheitsfunktionen für Unternehmensressourcen in der Amazon Cloud

- Aktivieren Sie mit einem Klick eine Check Point Virtual Appliance in der Amazon Cloud
- Wählen Sie die geeigneten Software Blades für Ihre Sicherheitsanforderungen aus

Einfache Verwaltung hybrider Umgebungen mit Cloud- und standortbasierten Sicherheitsfunktionen

- Verwalten Sie die Sicherheit Ihrer Cloud mit branchenführendem Sicherheitsmanagement
- Erstellen Sie mit einer Konsole eine Sicherheitsrichtlinie für Cloud- und standortbasierte Ressourcen
- Vereinfachen Sie Compliance und Auditing durch einheitliche Protokoll- und Berichterstellungsfunktionen

LEISTUNGSMERKMALE

Kompletter Schutz mit Check Point Software Blades

Mit der Check Point Virtual Appliance, einem Sicherheits-Gateway für die Amazon Cloud, können Sie alle Sicherheitsfunktionen der Check Point Software-Blade-Architektur nutzen. Die Firewall und IPS Software Blades schützen Services in der öffentlichen Cloud vor unberechtigten Zugriffen und Angriffen. Das Application Control Software Blade unterbindet Denial-of-Service-Angriffe auf Anwendungsebene und sichert Ihre Cloud-Services. Das IPsec VPN Software Blade sorgt für eine sichere Kommunikation mit Cloud-Ressourcen. Mit dem Mobile Access Software Blade können mobile Benutzer SSL-verschlüsselte Verbindungen zur Cloud herstellen. Dabei kommen Zwei-Faktor-Authentifizierung und Geräte-Pairing zum Einsatz. Das DLP Software Blade verhindert mit unserer einzigartigen User Check-Technology Datenverluste und unterstützt die benutzerbasierte Problemlösung in Echtzeit.

Schnelle Bereitstellung in zwei Schritten

Klicken Sie in Amazon Web Services einfach auf die virtuelle Check Point Appliance, um die relevanten Sicherheitsfunktionen der Software Blades zu aktivieren und Ihre Cloud-Ressourcen zu schützen.

Einheitliches Management für Cloud- und standortbasierte Infrastrukturen

Verwalten Sie die virtuelle Appliance in der Amazon Cloud mithilfe der vorhandenen standortbasierten Check Point Unified Security Management-Lösungen. Setzen Sie mithilfe der zentralen Konsole eine konsistente Sicherheitsrichtlinie für Unternehmensressourcen in der Amazon Cloud und für die standortbasierte Infrastruktur durch.

Sorgen Sie für Transparenz und Durchsetzung in der Cloud und für die standortbasierte Infrastruktur, indem Sie das Smart Event Software Blade verwenden. Vereinfachen Sie Compliance und Auditing mit einheitlichen Protokoll- und Berichterstellungsfunktionen.

Konfigurationstool für eine einfache Einrichtung der Virtual Appliance

Das Konfigurationstool für die Check Point Virtual Appliance können Sie auf Ihrem Laptop oder Computer ausführen. Es erstellt eine virtuelle private Cloud mit einem privaten Subnetz und startet darin eine Check Point Virtual Appliance. Dieser Prozess dauert weniger als eine Minute.

Anschließend können Sie eine Verbindung mit Ihrer neuen Virtual Appliance herstellen und die Lösung konfigurieren.

Virtual Appliance für Amazon Web Services

Sicherheit für virtuelle Umgebungen in der Amazon Cloud

INTERESSANT FÜR

- Kunden, die ihre outgesourcten Daten auf gewohntem Check Point-Niveau absichern wollen
- Kunden, die neben der Security ihrer Service Provider individuelle Sicherheitsanforderungen abdecken wollen (DLP, Application Control, IPS usw.)

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Sicherheit mit Software Blades

- Umfassende Sicherheitsfunktionen mit der Software-Blade-Architektur
- Schutz vor Netzwerkangriffen und Datenverlusten mit IPS und DLP Software Blades
- Sichere Cloud-Verbindungen von mobilen Anwendern und Benutzern im Unternehmen mit Mobile-Access- und VPN-Blades

Einheitliches Sicherheitsmanagement

- Einrichtung und Durchsetzung einheitlicher Richtlinien für Cloud- und standortbasierte Infrastrukturen
- Verwaltung von Cloud- und standortbasierten Richtlinien über eine zentrale Konsole
- Zusammengefasster Compliance-Bericht für Cloud- und standortbasierte Ressourcen
- Verwaltung von Änderungen an Sicherheitsrichtlinien mit dem SmartWorkflow Software Blade

Schnelle und einfache Bereitstellung

- Aktivieren Sie mit einem Klick eine Check Point Virtual Appliance in der Amazon Web Services
- Aktivieren Sie gewünschte Software Blades für den Schutz der Cloud
- Sorgen Sie für umfassende Sicherheit, auch wenn die Infrastruktur aufgrund der Elastizität der öffentlichen Cloud-Infrastruktur erweitert wird

Ideal für den Schutz von öffentlichen Cloud-Umgebungen

- Setzen Sie Sicherheitsrichtlinien des Unternehmens in Cloud-basierten Zweigniederlassungen um
- Isolieren Sie alte Anwendungen, die sich in der Cloud nur schwer sichern lassen und richten Sie spezielle Sicherheitsrichtlinien ein
- Duplizieren und sichern Sie wichtige IT-Ressourcen für die Notfallwiederherstellung

SPEZIFIKATIONEN

Check Point Virtual Security Appliance für Amazon Web Services
Virtuelle Appliance mit vollem Funktionsumfang der Check Point Software-Blade-Architektur

GESPRÄCHSEINSTIEG

- Wie planen Sie, Ihre öffentliche Cloud zu sichern?
- Machen Sie sich Sorgen über die Sicherheit von Verbindungen zwischen Hauptsitz und Zweigniederlassungen? Wie sind die Server gesichert?
- Wie wollen Sie Sicherheitsrisiken in der Cloud bewältigen (Netzwerkangriffe, Zugangskontrolle und Datensicherheit)?
- Wie möchten Sie für Ihre Cloud-Ressourcen Compliance-Berichte erstellen und Änderungen an Sicherheitsrichtlinien verwalten?
- Wie planen Sie, infizierte Ressourcen in der Cloud zu säubern oder zu isolieren?

Check Point

Security-Software-Blade-Lösungen

Security Gateway Software Blades

Die dynamische Software-Blade-Architektur bietet sichere, flexible und einfache Lösungen, die vollständig an die spezifischen Sicherheitsanforderungen eines jeden Unternehmens und jeder Umgebung angepasst werden können.

Firewall
IPsec VPN
IPS
Web Security
URL Filtering
Antivirus & Anti-Malware
Antispam & E-Mail Security
Advanced Networking
Acceleration & Clustering
Voice over IP
Data Loss Prevention

Check Point ThreatCloud™

Echtzeitschutz zur Bekämpfung der Internetkriminalität

Die ThreatCloud™ liefert den Software Blades Echtzeit-Sicherheitsinformationen aus dem ersten gemeinsamen Netzwerk zur Bekämpfung von Cyberkriminalität.

- Erstes gemeinsames Netzwerk zur Bekämpfung von Cyberkriminalität mit:
  - über 250 Mio. analysierten Adressen zur Bot-Erkennung
  - über 4,5 Mio. Malware-Signaturen
  - mehr als 300.000 Malware-infizierten Webseiten
- Dynamische Updates über ein weltweites Netzwerk an Sensoren zur Erkennung von Bedrohungen
- Echtzeitschutz-Informationen für Bereitstellung auf Ihren Gateways

Firewall Software Blade

ÜBERSICHT

Das Check Point Firewall Software Blade bietet die Funktionalität der bewährtesten Firewall der Branche – 100 Prozent aller Fortune-100-Unternehmen vertrauen darauf. Basierend auf einer patentierten adaptiven und intelligenten Inspektionstechnologie, sichert das Firewall Blade über 200 Anwendungen, Protokolle und Dienste und bietet umfassenden Schutz vor Angriffen sowohl für die Anwendungs- als auch für die Netzwerksicherheit.

VORTEILE

- Schützt geschäftskritische Anwendungen durch umfassende Netzwerk- und Anwendungssicherheit
- Verhindert unerlaubte Netzwerkzugriffe mit ausgefeilter, auf patentierter Stateful-Inspection-Technologie basierender Zugriffskontrolle
- Erstklassige Leistung mit hohem Datendurchsatz durch die Firewall
- Höchste Flexibilität bei der Bereitstellung durch Multi-Plattform-Unterstützung

*Leistungsdaten können variieren. Die neuesten Daten finden Sie auf der Check Point-Website.

LEISTUNGSMERKMALE

- Zugriffskontrolle stellt sicheren Zugriff auf Clients, Server und Anwendungen sicher
- Authentifizierung stellt Identität der Benutzer sicher und garantiert, dass diese zum Netzwerkzugriff autorisiert sind
- Network Address Translation (NAT) verarbeitet routingfähige und nicht routingfähige reale Netzwerkadressen, die aus Sicherheitsgründen verschleiert wurden
- ISP-Redundanz stellt zuverlässige Internetkonnektivität sicher, indem einzelne Sicherheits-Gateways oder Cluster aus Gateways über mehrere redundante ISP-Links mit dem Internet verbunden werden
- Bridge-Modus untersucht den Datenverkehr und verwirft oder blockiert nicht autorisierten oder als unsicher erachteten Datenverkehr, während erlaubter Datenverkehr von einer Schnittstelle zur nächsten passieren darf, ohne dass dabei das ursprüngliche IP-Routing beeinträchtigt wird

INTERESSANT FÜR

- Unternehmen jeder Größe

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Branchenführende Firewall
- Schützt 100% der Fortune-100-Unternehmen
- Beinhaltet eine Vielzahl patentierter Technologien, darunter auch Stateful Inspection
- Höchste Flexibilität dank Multi-Plattform-Unterstützung und verschiedenster Bereitstellungsoptionen

GESPRÄCHSEINSTIEG

- Die Check Point-Firewall ist die führende Firewall der Branche.
- Die Check Point-Firewall schützt 100 Prozent der Fortune-100-Unternehmern.

Firewall Software Blade

SPEZIFIKATIONEN

Funktion	Beschreibung
Protokoll-/ Anwendungsunterstützung	Schützt über 200 Anwendungen und Protokolle
VoIP Protection	Unterstützt SIP, H.323, MGCP und SIP mit NAT
Network Address Translation	Unterstützt Static/Hide NAT mit manuellen oder automatischen Regeln
DHCP Gateways	Sicherheits-Gateways können mit dynamischer IP-Adresse betrieben werden
VLAN	Bis zu 256 VLANs
Link Aggregation	802.3ad passiv und 802.3ad aktiv (spezielle Version)
Bridge Mode/Transparent Mode	Unter SecurePlatform für Schnittstellenpaare unterstützt
Erweiterter Satz von Richtlinienobjekten	Objekte für individuelle Knoten, Netzwerke und Gruppen sowie dynamische Objekte
IP-Versionen	IPv4 und IPv6
Schutzmaßnahmen bei Ausfall	Standardfilter schützt während des Systemstarts und vor der erstmaligen Richtlinienkonfiguration
Secure Internal Communications (SIC)	Zertifikatbasierter, sicherer Kommunikationskanal zwischen allen verteilten Check Point-Komponenten, die ein und derselben Managementdomäne angehören
Authentifizierung	
Benutzer- und rollenbasierte Firewall-Regeln	Benutzer-, Client- und Sitzungsauthentifizierung
Lokale Benutzer	Lokaler Datenbank-Benutzerspeicher integriert
RADIUS und RADIUS-Gruppen	Mehrere Server und MS-CHAPv2- sowie MS-PAP-Methode
LDAP und LDAP-Gruppen	Microsoft Active Directory, Novell Directory Server, Netscape Directory Server, OPSEC-zertifizierte LDAP-Server
TACACS+	Unterstützt
RSA SecurID	Unterstützt
Interne CA	Enthalten
Anpassbare Authentifizierungsnachrichten	Unterstützt
Schema-Erweiterung	Unterstützt
Verzeichnismanagement	Verfügbar über grafische Benutzeroberfläche

IPsec VPN Software Blade

ÜBERSICHT

Das Check Point IPsec VPN Software Blade integriert Zugriffskontrolle, Authentifizierung und Verschlüsselung und stellt so die Sicherheit von Verbindungen über das Internet sicher. Es bietet sichere Konnektivität für Unternehmensnetzwerke, mobile Mitarbeiter und Mitarbeiter an entfernten Standorten, Zweigstellen und Geschäftspartner.

VORTEILE

- Einfaches, zentrales Management von Remote Access und Site-to-Site-VPNs
- Erweiterte IPsec-VPN-Sicherheit
- Verschiedene Konnektivitätsmodi für Remote Access VPN bietet Unterstützung für alle Arten von Standorten und Netzwerken

LEISTUNGSMERKMALE

- Mit der einheitlichen Oberfläche können Administratoren beteiligte Gateways für weitverzweigte, große VPN-Szenarien festlegen. Außerdem ermöglicht die integrierte CA (Certificate Authority) die Verwaltung der Schlüssel durch die schnelle Konfiguration von Stern- und Mesh-Topologien
- Mit Hilfe der verschiedenen Methoden zur VPN-Erstellung können Administratoren beim Aufbau routenbasierter VPNs für komplexe, weitläufige, dynamische Umgebungen die Verschlüsselungsregeln für den VPN-Datenverkehr festlegen und Domain-basierte VPNs für Datenverkehr hinter dem Gateway einrichten
- Die erweiterte IPsec VPN-Sicherheit schützt das VPN vor Denial-of-Service-Angriffen auf das Internet-Key-Exchange-Protokoll und gestattet Administratoren die Anpassung der Sicherheitsrichtlinien in Abhängigkeit von der Art des Datenverkehrs
- Die flexible Unterstützung für den Fernzugriff umfasst eine Reihe verschiedener VPN-Client-Optionen, so dass Administratoren eine Lösung entwerfen können, die ihren Anforderungen an den Fernzugriff bestmöglich entspricht
- Verschiedene VPN-Konnektivitätsmodi für Fernzugriff ermöglichen eine Vielzahl unterschiedlicher Anforderungen für die Remote-Benutzerkonnektivität sowie unterschiedliche Routing-Bedürfnisse

INTERESSANT FÜR

- Fast alle Unternehmen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Branchenführendes IPsec-VPN
- Umfassende Bereitstellungsoptionen, darunter Topologie-, routenbasiertes, IPsec- und Fernzugriffs-VPNs
- Einfaches VPN-Management per Mausklick

GESPRÄCHSEINSTIEG

- Das Check Point VPN Software Blade ist weltweit als führend im VPN-Bereich anerkannt.
- 100 Prozent aller Fortune-100-Unternehmen vertrauen auf den Check Point VPN Software Blade.

IPsec VPN Software Blade

SPEZIFIKATIONEN

Funktion	Beschreibung
Authentifizierungsmethoden	Kennwort, RADIUS, TACACS, X.509 und SecurID
Certificate Authority	Integrierte X.509-Certificate Authority
VPN-Communitys	Konfiguriert beim Erstellen von Objekten automatisch Site-to-Site-Verbindungen
Unterstützte Topologien	Stern und Mesh
Routenbasiertes VPN	Nutzt virtuelle Tunnelschnittstellen und nummerierte/nicht nummerierte Schnittstellen
VPN-Resiliency	Multiple Entry Point (MEP) und Wire-Modus
VPN-Routeninjektion	Routeninjektionsmechanismus (RIM)
Site-to-Site-VPN-Modi	Domänenbasiert und routenbasiert
Direktionales VPN	Durchsetzung zwischen Communitys oder innerhalb der Community
IKE (Phase 1)-Schlüsselaustausch	AES-256, 3DES, DES und CAST
IKE (Phase 1)-Datenintegrität	MD5, SHA1
IPsec (Phase 2)-Datenverschlüsselung	3DES, AES-128, AES-256, DES, CAST, DES-40CR, CAST-40 und NULL Algorithmus
IPsec (Phase 2)-Datenintegrität	MD5 und SHA1
IKE (Phase 1)- und IPsec (Phase 2)-Diffie-Hellman-Gruppen	Gruppe 1 (768 Bit), Gruppe 2 (1024 Bit), Gruppe 5 (1.536 Bit) und Gruppe 14 (2.048 Bit)
IKE (Phase 1)-Optionen	Aggressive Mode
IPsec (Phase 2)-Optionen	Perfekte Transportvertraulichkeit und IP-Kompression
Unterstützung für mobile Geräte	SecureClient Mobile für Windows Mobile, L2TP-Unterstützung für iPhone
Mehrere IPsec-VPN-Clients	Check Point Endpoint Security, Endpoint Security VPN R75, SecuRemote

Mobile Access Software Blade

ÜBERSICHT

Das Check Point Mobile Access Software Blade ist eine sichere und einfache Lösung, um Smartphones, Tablets und PCs über das Internet mit Unternehmensanwendungen zu verbinden. Die Lösung bietet mittels Layer-3 VPN- und SSL VPN-Fernzugriff der Enterprise-Klasse, sodass Sie bequem und sicher auf E-Mail, Kalender, Kontakte un Unternehmensanwendungen zugreifen können.

VORTEILE

Einfache Verbindung über mobile Geräte

- Sichere Anbindungsmöglichkeit von Smartphones, Tablets, PCs und Laptops
- Client- und webbasierte VPN-Verbindungen
- Einfacher Zugriff für mobile Mitarbeiter mit verwalteten oder nicht verwalteten Geräten

Sorgt für den Schutz Ihrer Daten

- Sichere Kommunikation Dank bewährter Verschlüsselungstechnologien
- Verifizierung autorisierter Benutzer mit Zwei-Faktor-Authentifizierung
- Schutz von Daten auf gestohlenen oder verloren gegangenen Geräten dank Gerätesperrung und Fernlöschung

Einheitliches Management für einfache Bereitstellung und Verwaltung

- Umfassende Integration in den Check Point Security Policy Manager
- Aktivierung von Benutzerzertifikaten mit einem Klick
- Bereitstellung und Konfiguration des Mobile Access Software Blade auf Ihrem vorhandenen Sicherheitsgateway (VPN Blade wird auf dem Gateway vorausgesetzt!)

LEISTUNGSMERKMALE

Das Mobile Access Software Blade bietet:

- Sicheren SSL VPN-Zugang
- Zwei-Faktor-Authentifizierung
- Pairing von Geräten/Endbenutzern
- Mobiles Unternehmensportal
- Interaktion mit Security Blades inklusive IPS, Anti-Malware und Firewall

Verbindungsoptionen:

- Check Point Mobile-App
- SSL VPN-Portal über einen Browser
- SSL Network Extender (SNX)

INTERESSANT FÜR

- Jede Unternehmensgröße
- Finanzdienstleister, Behörden, Unternehmensdienstleister, Gesundheitswesen und Industrie
- Kunden, deren Mitarbeiter über ihre mobilen Geräte sicher auf Unternehmensdaten zugreifen sollen
- Kunden, die sich eine sicherere Lösung für den Zugriff auf Unternehmensressourcen mit mobilen Geräten wünschen
- Kunden, die bereits ein Check Point Gateway besitzen
- Primäre Entscheidungsträger: CSO, Security VP/Director innerhalb von Netzwerk- und/oder Desktop-Administrations-gruppen
- Wichtige Beeinflusser: CIO, VP/Director/Manager für IT, IS, MIS, Desktop- und Netzwerkgruppen; Mitarbeiter, die sich Zugriff auf Unternehmensressourcen mit ihren mobilen Geräten wünschen

LEISTUNGSMERKMALE

Sicherheit

- Nutzeridentität und Geräte werden miteinander verknüpft
- Sicherung der E-Mail-Synchronisation mit ActiveSync

Benutzerfreundlichkeit

- Einfacher Zugriff auf das Unternehmensportal
- Einheitliche Benutzeroberfläche
- Stets verfügbarer Zugang zu E-Mails

Geringere Kosten und einfache Verwaltung

- Einfaches Software Blade Add-on (2012er Appliances werden mit einem 5 User Mob Blade ausgeliefert)
- Nutzung des Gateways für zusätzliche Netzwerksicherheits-funktionen wie Firewall und IPS
- Konsolidierung von SSL VPN- und IPSec VPN-Lösungen auf einem Gateway

GESPRÄCHSEINSTIEG

- Welche Herausforderung sehen Sie darin, einer Vielzahl von Mobilgeräten den Zugriff auf Ihre Unternehmensdaten zu gestatten?
- Welche Compliance-Richtlinien hat Ihr Unternehmen hinsichtlich des Zugangs für mobile Geräte implementiert?
- Fühlen Sie sich hinsichtlich mobiler Geräte und deren Zugriff auf Ihre Unternehmens-E-Mail ausreichend gesichert?

Mobile Access Software Blade

SPEZIFIKATIONEN

Check Point Mobile Application: Web Portal-Spezifikation		
iOS	3.1.3 und höher	
Android	2.1 und höher	
Windows	XP, Vista, Windows Layer-3 VPN-Client	
Check Point Mobile VPN Client – Layer-3 VPN	Stern und Mesh	
iOS	5.0 und höher	
SSL VPN-Portal	Multiple Entry Point (MEP) und Wire-Modus	
Internet Explorer	5.5 und höher	
Firefox	1.0.3 und höher	
Safari	Alle	
Gateway-Spezifikation		
Hardware	• Check Point 2200, 4000, 12000, 21400 und 61000 Appliances • Check Point Power-1 • Check Point UTM-1 • Check Point IAS • Alternativ als dedizierte Appliance Appliance for Mobile Access (enthält Firewall, VPN, Advanced Networking & Clustering, Identity Awareness und Mobile Access). Inkl. Lokalem Management mit User Directory für bis zu 2 Gateways - 12600 für unlimited Concurrent User (max. 10.000 CCU empfohlen) - 4800 für unlimited Concurrent User (max. 2.500 CCU empfohlen) - 2200 für 200 Concurrent User	
Betriebssystem	• GAiA R75.40 oder höher • SecurePlatform R71.30 oder höher • Check Point Mobile VPN setzt R71.50 oder höher voraus	
Management Platform-Spezifikationen*		
Check Point	• GAiA • SecurePlatform • IPSO 6.2 (festplattenbasiert)	
Windows	Server 2003/2008 32-Bit	
Linux	RHEL 5.0/5.4 32-Bit	
Sun/Oracle (SPARC)	Sun Solaris 8, 9, 10	
Client-Gerät	Betriebssystem	Browser
PC	Windows 7 32/64-Bit, Vista 32/64-Bit, XP 32-Bit	Internet Explorer 5.5 und höher, Firefox 1.0.3 und höher
Mac	Mac 10.4 und höher	Safari
Linux	Fedora 8, Ubuntu 7, RHEL 3.0, Suse 9 und höher, Red Hat 7.3	Firefox 1.0.3 und höher

*Security Management Server R71.10 erforderlich

IPS Software Blade

ÜBERSICHT

Das Check Point IPS Software Blade bietet vollständige Funktionen zur Abwehr von Eindringlingen bei Multi-Gigabit-Übertragungsraten und ermöglicht damit erstklassige Leistung bei kompletter Sicherheit. Es kombiniert die Bereitstellungs- und Managementvorteile einer integrierten Lösung mit einer Leistung, welche die dedizierten Intrusion-Prevention-Systeme übertrifft.

VORTEILE

- Kombiniert Spitzentechnologien zu einem akkuraten Schutz vor Bedrohungen in einem einzigen Gateway und senkt gleichzeitig die laufenden Betriebskosten
- Sorgt für branchenführende Leistung der Firewall- und IPS-Funktionen für höchsten Datendurchsatz bei unglaublichen Einsparungen – und das ohne Kompromisse bei der Sicherheit
- Bietet bis zu 10-fache Leistung gegenüber bereits vorhandenen integrierten Sicherheits-Gateways mit IPS-Funktionen und bis zu 22-mal höhere Leistung bei über 2.000 aktivierten Sicherheitsfunktionen
- Enthält vollständige Palette von Managementtools zur Reduzierung des Managementaufwands und zur zeitnahen Bereitstellung proaktiver Schutzmaßnahmen
- Schützt auch zwischen Patches, indem Sicherheitsmaßnahmen bei Verzögerungen im Patch-Vorgang verstärkt werden
- Integrierte IPS-Funktionen zur Reduzierung der Hardware- und Softwarekosten, zur Einsparung von Platz im Rack und damit verbundenen Kosten, Vereinfachung des Managements und Verringerung der Latenz des Datenverkehrs
- Bietet Schutz vor Eindringlingen mit einem Klick für sofortigen IPS-Schutz und einen schnellen Return on Investment

LEISTUNGSMERKMALE

- Vollständige Intrusion-Prevention-Funktionalität sorgt für umfassenden Schutz vor böswilligem Datenverkehr im Netzwerk. Dies wird durch den Einsatz präventiver, exakter Verteidigungsmaßnahmen erreicht, die vom Check Point Update Service in Echtzeit aktualisiert werden
- Branchenführende Gesamtsystemleistung durch Analyse nur des für Angriffe relevanten Datenverkehrs, was den Aufwand reduziert und die Genauigkeit erhöht
- Reibungslose Bereitstellung durch Nutzung bereits vorhandener Sicherheitsinfrastruktur, wodurch Bereitstellungszeit und -kosten reduziert werden
- Das dynamische Bedrohungsmanagement aktiviert in Abhängigkeit von konfigurierbaren Parametern automatisch neue Schutzfunktionen, und die konfigurierbare, verfolgbare Überwachung zeichnet Ereignisse mittels anpassbarer, detaillierter Berichte und Protokolle auf
- Präventive Sicherheitsaktualisierungen kombinieren die zuverlässigen IPS-Funktionen mit einer konzertierten Patching-Strategie, so dass Netzwerkadministratoren das Netzwerk zwischen Upgrades und Patches sichern können

INTERESSANT FÜR

- Unternehmen, die bereits vorhandene Sicherheits-Gateways und -Infrastruktur zur Bereitstellung von IPS nutzen wollen
- Unternehmen, die aufgrund befürchteter Leistungseinbußen vor der Bereitstellung integrierter IPS zurückschrecken
- Unternehmen, die Check Point R70 oder neuer einsetzen und IPS-Schutz hinzufügen möchten, ohne eine neue Appliance zu erwerben
- Kunden, die Check Point R65 oder frühere Versionen einsetzen und am erweiterten IPS-Schutz und den Managementfunktionen des IPS Software Blades interessiert sind und auf R70 aktualisieren möchten

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Multi-Gigabit-Gesamtsystemleistung bei Firewall und IPS
- Senkung der Hard- und Software-Kosten, des benötigten Platzes im Rack und damit verbundener Kosten durch Konsolidierung eigenständiger Lösungen
- Bietet bestmöglichen Schutz für Schwachstellen von Microsoft-Produkten
- Enthält präventive Schutzmaßnahmen, die schon vor der Verbreitung von Exploits wirken
- Einfache Bereitstellung und kontinuierliches Management
- Untersuchung des Datenverkehrs erfolgt einmalig sowohl für Firewall als auch IPS

GESPRÄCHSEINSTIEG

- Wie schnell und wie häufig installieren Sie oder Ihr Unternehmen Sicherheitspatches von Herstellern oder Patches zur Fehlerbehebung?
- Suchen Sie eine Sicherheitslösung, die Ihr Netzwerk vor Bedrohungen und Angriffen schützt?
- Haben Sie schon einmal ungeplante Ausfallzeiten geschäftskritischer Anwendungen aufgrund von Netzwerkeinbrüchen erlebt?

IPS Software Blade

SPEZIFIKATIONEN

Funktion	Beschreibung
Leistung	
Integrierte IPS-Leistung	Bis zu 15 Gbit/s
Schwellwert für Gateway-Auslastung	Schützt die Firewall-Leistung unter Last durch einen konfigurierbaren Software-Bypass
Sicherheit	
Multifunktions-Erkennungsmodul	• Schwachstellen- und Exploit-Signaturen • Protokollvalidierung • Erkennung von Anomalien • Verhaltensbasierte Erkennung • Korrelation mehrerer Elemente
Abdeckung von Microsoft-Schwachstellen	Erster Platz bei Microsoft-Schutzmechanismen im Jahr 2008
Unterstützung des Patch-Prozesses	Schützt Ihr Netzwerk vor Angriffen, während Hersteller-Patches angewendet werden
Echtzeitschutz	Schutzaktualisierungen für: • Client- und Serverschwachstellen • Exploits • Protokollmissbrauch • Ausgehende Malware-Kommunikation • Tunneling-Versuche • Anwendungskontrolle • Allgemeine Angriffsarten ohne vordefinierte Signaturen • Präventive Sicherheitsfunktionen
Application Intelligence	Schutz und Kontrolle von Anwendungen, inklusive Instant Messaging- und Peer-to-Peer-Programmen
Offene Signaturen	Erstellen Sie eigene Signaturen in einer offenen Signatursprache.
Anti-DoS-Modul	Erweiterter Schutz vor Denial-of-Service-Angriffen
Bereitstellung	
Profile	Verringerter Administrationsaufwand durch Anwendung derselben Schutzmaßnahmen auf Gruppen von Systemen
Vordefinierte Profile	Sofort einsetzbare, auf Sicherheit oder auf Leistung optimierte Schutzprofile
Nur-Erkennungs-Modus	Ermöglicht die Erkennung von böswilligem Verkehr durch Ihre vorhandenen Schutzsysteme, der Verkehr wird jedoch nicht blockiert.
Sandbox für neue Schutzfunktionen	Bietet eine Sandbox-Umgebung zum Ausprobieren neuer Schutzfunktionen, ohne das Netzwerk zu beeinträchtigen.
Management	
Aktivierungsregeln	Aktivierung von Schutzmaßnahmen je nach: • Schweregrad der Bedrohung • Beeinträchtigung der Leistung • Vertrauensstufe der Schutzfunktion
Packet Capture	Sammeln Sie Datenverkehr für detaillierte forensische Analysen.
Verfolgung	Markieren Sie Schutzfunktionen zur späteren Analyse.
Zeitleistenansicht	Konfigurieren Sie einfach benutzerdefinierte Ansichten dessen, was für Sie wirklich wichtig ist (z. B. Sicherheitsvorfälle bei Ihren wichtigen Netzwerksystemen).
Systemübersicht	Status des IPS-Systems auf einen Blick
Einheitliches Management	Verwalten Sie integrierte und eigenständige IPS über eine einzige Oberfläche.
Netzwerkausnahmen	Erstellen Sie Ausnahmen für die Schutzfunktionen.
Weitere Informationen zur Schutzfunktion	Bietet detaillierte Informationen zu jeder Schutzfunktion, inklusive: • Schwachstellen- und Bedrohungsbeschreibungen • Schweregrad der Bedrohung • Beeinträchtigung der Leistung • Vertrauensstufe

Application Control Software Blade

ÜBERSICHT

Das Check Point Application Control Software Blade bietet Unternehmen jeder Größe ein Höchstmaß an Anwendungssicherheit und Identitätskontrolle. Auf Grundlage von Benutzern oder Gruppen können granulare Richtlinien definiert werden und so die Nutzung von über 240.000 Web-2.0-Anwendungen und Widgets analysiert gesperrt oder deren Nutzung beschränkt werden.

VORTEILE

- Transparenz und Kontrolle bei Web-2.0-Anwendungen und Social-Network-Widgets
- Identifizieren, sperren oder einschränken der Nutzung von Anwendungen nach Benutzern, Gruppen oder Geräten
- UserCheck-Technologie informiert Mitarbeiter über Einschränkungen beim Anwendungszugriff und liefert gleichzeitig Informationen zu den Nutzungsrichtlinien des Unternehmens.
- Analyse von SSL-verschlüsseltem Datenverkehr

LEISTUNGSMERKMALE

Granulare Anwendungskontrolle

- Überwacht die Verwendung von Web-2.0-Anwendungen nach Benutzern, Gruppen oder Geräten
- Informiert Benutzer über Zugangs- und Nutzungsrichtlinien

Appwiki-Anwendungsdatenbank

- Große Datenbank mit Web-2.0-Anwendungen und Social-Network-Widgets
- Über 80 Kategorien inklusive Web 2.0, IM, P2P und Dateifreigaben (File Sharing)

Integriert in die Check Point Software-Blade-Architektur

- Einfache Bereitstellung mit nur einem Klick
- Einheitliche Verwaltung über eine zentrale Konsole
- Bequeme Erstellung und Verwaltung granularer, identitätsbasierter Sicherheitsrichtlinien

INTERESSANT FÜR

- Mittelständische und große Unternehmen
- Finanzdienstleistungen, Behörden, Gesundheitswesen und Industrie
- Unternehmen, die strenge gesetzliche Vorgaben einhalten müssen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Integriert in die Software-Blade-Architektur
- Extrem granulare Richtliniendefinitionen
- Nutzung von Anwendungen ermitteln, zulassen, sperren, anfragen und einschränken

GESPRÄCHSEINSTIEG

- Wie transparent ist die Web-2.0-Nutzung in Ihrem Netzwerk heute?
- Wie steuern Sie, wer Zugriff auf Anwendungen erhält und wie diese Anwendungen genutzt werden?
- Wie sorgen Sie für die Bereitstellung und Durchsetzung von Nutzungsrichtlinien für Ihre Benutzer?
- Wie weisen Sie einzelnen Benutzern verschiedene Berechtigungen zu?
- Wie viel kostet Sie die Verwaltung der Netzwerkbandbreite sowie die Unterstützung nicht genehmigter Anwendungen? Wie viel kostet Sie die von nicht genehmigten Anwendungen verursachte Einschränkung der Produktivität?
- Wie schützen Sie Ihr Netzwerk vor anwendungsbasierten Bedrohungen? Wie könnten Sie den Schutz verbessern?
- Sind sich Ihre Benutzer der Risiken bewusst? Wie können Sie sie effektiv schulen?

SPEZIFIKATIONEN

Unterstützte Appliance-Familien	Unterstützte Betriebssysteme
• Check Point 2200, 4000, 12000, 21400 und 61000 Appliances • Check Point Power-1 • Check Point IP Appliances • Check Point UTM-1 • Check Point IAS	• GAiA • SecurePlatform • IPSO 6.2 Disk-based • IPSO 6.2 Flash-based • Windows

URL Filtering Software Blade

ÜBERSICHT

Das Check Point URL Filtering Software Blade lässt sich in das Application Control Software Blade integrieren und sorgt für eine einheitliche Verwaltung und Durchsetzung aller Aspekte der Websicherheit. URL Filtering sorgt durch die vollständige Integration in das Gateway für optimierte Websicherheit. Ein externer Proxy ist nicht erforderlich. Richtlinien werden mit Application Control durchgesetzt, um umfassenden Web- und Web-2.0-Schutz zu bieten. Zudem ist eine Einbeziehung der Nutzer über User Check möglich.

VORTEILE

Schutz der Benutzer durch Cloud-basierte Kategorisierung und UserCheck-Technologie

- Dynamische Cloud-basierte Datenbank mit über 100 Millionen Webseiten
- Echtzeitaktualisierung für geänderte und neue URLs
- UserCheck schult Benutzer mit Echtzeit-Warnungen zu Webrichtlinien

Vollständige Integration in Application Control für eine sichere Webnutzung

- Einheitliche Verwaltung und Durchsetzung aller Aspekte der Websicherheit
- Festlegung, Durchsetzung und Berichterstellung für Web- und Anwendungssicherheitsrichtlinien auf Benutzer- und Gruppenebene
- Kontrolle von über 100 Millionen Webseiten, 4.500 Web-2.0-Anwendungen und 225.000 Widgets

Optimale Sicherheit und geringere Gesamtbetriebskosten

- Keine Umgehung mit externen Proxys dank vollständiger Integration von URL Filtering in CheckPoint-Gateways
- Durchsetzung der Prüfung des gesamten Datenverkehrs – auch bei Nutzung von Nicht-Standard-Ports
- Prüfung von SSL-verschlüsseltem Datenverkehr im Gateway
- Aktivierung mit einem Klick auf Grundlage der Software-Blade-Architektur
- Bis zu 90 % geringere Gesamtbetriebskosten im Vergleich zu einer herkömmlichen Einzellösung

LEISTUNGSMERKMALE

- Einheitliche Lösung zum URL Filtering- und zur Kontrolle von Applikationen
- Dynamische Cloud-basierte Kategorisierung
- Zugriff auf über 100 Millionen kategorisierte Webseiten
- Analyse von verschlüsseltem Datenverkehr
- Einbeziehung und Schulung von Benutzern mit UserCheck

INTERESSANT FÜR

- Mittelständische und große Unternehmen
- Finanzdienstleister, Behörden, Bildung, Gesundheitswesen und Industrie
- Unternehmen, die strenge gesetzliche Vorgaben einhalten müssen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Vollständige Integration von URL Filtering und Application Control

- Schutz von Web 2.0, Blogs und sozialen Netzwerken
- Bequeme Verwaltung einheitlicher Richtlinien
- Verwaltung, Durchsetzung und Berichterstellung (auch für einzelne Benutzer)

Cloud-basierte Kategorisierung und UserCheck-Technologie

- Dynamische Aktualisierungen von über 100 Millionen Webseiten
- Echtzeitbasierte Ermächtigung und Schulung von Benutzern zu Web-Nutzungsrichtlinien

Lösung der Enterprise-Klasse mit umfassender Integration in Check Point-Gateways

- Vermeidung von Bypass-Verfahren
- Skalierung bis zu einem Durchsatz von 7 Gbit und 5 Millionen gleichzeitigen Sitzungen
- Granulare Kontrolle über Benutzer und Anwendungen
- Hochverfügbarkeits-Clustering

GESPRÄCHSEINSTIEG

- Wie geht Ihre vorhandene URL-Filtering-Lösung mit Anwendungen wie Skype um?
- Wie verwalten Sie verschiedene Einzellösungen wie URL Filtering, Application Control, Firewall und IPS?
- Wie schützen Sie Ihr Netzwerk vor webbasierten Bedrohungen? Wie könnten Sie den Schutz verbessern?
- Welche Probleme haben Sie mit Ihrer vorhandenen URL-Filtering-Einzellösung? Wie sieht es mit der Benutzerfreundlichkeit und den Gesamtbetriebskosten aus?
- Wie können Sie in Ihrer Umgebung Web-2.0-Inhalte filtern?

SPEZIFIKATIONEN

Unterstützte Appliance-Familien	Unterstützte Betriebssysteme
• Check Point 2200, 4000, 12000, 21400 und 61000 Appliances • Check Point Power-1 • Check Point IP Appliances • Check Point UTM-1 • Check Point IAS	• GAiA • SecurePlatform • IPSO 6.2 Disk-based • IPSO 6.2 Flash-based • Windows

Anti-Bot Software Blade

ÜBERSICHT

Das Anti-Bot Software Blade von Check Point wurde speziell entwickelt, um Bots zu enttarnen und zu stoppen. Die Lösung basiert auf Check Points Multi-Tier ThreatSpect™-Technologie, die Unternehmen dabei hilft, Gefahrer aufzudecken, abzuwenden und künftigen Angriffen vorzubeugen. Multi-Tier ThreatSpect™ ist eine einzigartige Detection-Engine, die den Datenverkehr auf jedem Gateway analysiert, Gefahrenausbrüche identifiziert und Bots aufdeckt, indem sie eine Vielzahl von Risikofaktoren miteinander korreliert – etwa Botnet-Muster und -Profile, die Verstecke entfernter Betreiber und die Verhaltensweisen von Attacken. Wurde ein Bot identifiziert, kann das Unternehmen über intuitive Dashboards schnell feststellen, welches Risiko für die Geschäftsabläufe besteht – etwa durch Datenverlust oder betrügerische Spam-Software.

VORTEILE

- Erkennen von Bots auf Ihren Rechnern
- Stoppt „Advanced Persistant Threat“-Attacken
- Verhindert Datendiebstahl durch Bots
- Auf Basis der ThreatCloud stets aktualisierte Datenbank
- Einfaches Erkennen von Infektionen, Ermittlung des Schadens sowie Entscheidungshilfe für das weitere Vorgehen.

LEISTUNGSMERKMALE

- Erkennt und stoppt Bots noch bevor sie Ihr Netzwerk erreichen
- Einheitliches Management und Reporting für Antivirus und Anti-Bot
- Für jedes Check Point Gateway verfügbar
- Umfassende Datenbank zur schnellen Erkennung von Bots auf Basis der ThreatCloud
- Erkennung von Bots mit Hilfe der Kombination unterschiedlicher Techniken, wie der Reputation von IP-Adresse, URLs und DNS-Adresse, Verhaltensmustern und dem Scan von Bot-Aktivitäten

INTERESSANT FÜR

- Unternehmen jeder Branche
- Unternehmen jeder Größe

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

In ThreatCloud Real-Time Intelligence

- Umfassende Sicherheit auf Basis einer mehr als 250 Millionen großen Adressdatenbank
- Dynamische Ergänzung von neuen Bots durch weltweilt verteilte Sensoren
- Echtzeit-Aktualisierung Ihres Gateways

GESPRÄCHSEINSTIEG

- Wissen Sie über Bots und Bot-Netze Bescheid, die Ihrem Unternehmen gefährlich werden können?
- Verschicken Ihre Endgeräte Spam?
- Wie identifizieren Sie in Ihrem Unternehmen durch Bots infizierte Endgeräte?
- Wie würde Datenverlust, der durch Bots zustande kommt, sich auf Ihr Unternehmen auswirken?
- Wie viel Zeit kostet es Sie, Infektionen zu erkennen und zu bereinigen?

SPEZIFIKATIONEN

Supported Appliance Families	Supported Operating Systems
• Check Point 2200, 4000, 12000, 21400 and 61000 Appliances • Check Point Power-1 • Check Point IP Appliances • Check Point UTM-1 • Check Point IAS	• GAiA • SecurePlatform • IPSO 6.2 Disk-based • Windows

Antivirus Software Blade

ÜBERSICHT

Eine weitere Verstärkung für Check Points umfassende Gefahrenprävention ist das weiter entwickelte Antivirus Software Blade, das ebenfalls von der ThreatCloud mit Informationen versorgt wird. Die neue Antivirus-Lösung bietet 300-mal mehr Signaturen als ihre Vorgängerversionen. Sie ermöglicht Unternehmen, den Zugriff auf Malware-infizierte Websites einzudämmen und ihre Host-Systeme vor unbekannten Virus-Infektionen, die sich über das Netzwerk einschleichen, zu schützen. Über intuitive Dashboards können die Anwender Bot- und Malware-Bedrohungen schnell analysieren und auftretende Gefahren sowie deren Risiko-Level herausstellen und daraus resultierende Sicherheitsauswirkungen für das Unternehmen aufzeigen – wie zum Beispiel Datenverlust oder eine Zunahme an betrügerischem Spam-Aufkommen.

VORTEILE

- Schutz von Schäden durch Malware bereits am Gateway
- Jederzeit aktuelle Datenbank auf Basis von ThreatCloud, die mehr als 300-mal so viele Signaturen enthält als frühere Versionen
- Erkennung bislang unbekannter Malware über die Prüfung von verdächtigen Dateien innerhalb einer sicheren Umgebung

LEISTUNGSMERKMALE

- ThreatCloud Datenbank mit mehr als 250 Millionen auf Bots analysierten Adressen, 4,5 Millionen Malware-Signaturen und 300.000 bedrohlichen Webseiten
- Antivirus auf bestehende Gateways
- Sofort verfügbarer Schutz
- Einmalige Zusammenarbeit mit dem Anti-Bot Blade

INTERESSANT FÜR

- Alle Unternehmen
- Unternehmen, deren Peers durch Viren oder Malware beeinträchtigt wurden
- Unternehmen, die gesetzliche Vorschriften wie HIPAA einhalten müssen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- 300-mal umfassendere Signatur-Datenbank als in vorherigen Versionen
- Schützt vor Zugriff von durch Malware infizierten Webseiten
- Kombination mit den Anti-Bot Blade

GESPRÄCHSEINSTIEG

- Wie schützen Sie Ihr Unternehmen vor Advanced Persistent Threats (APTs)?
- Wie identifizieren Sie in Ihrem Netzwerk Bots?
- Wie geht Ihre aktuelle Lösung mit der ständig wachsenden Anzahl von Viren, Würmern, Trojanern und Bots um?
- Wie viel Zeit kostet es Sie, Infektionen zu erkennen und aus dem Netzwerk zu löschen?

SPEZIFIKATIONEN

Unterstützte Appliance-Familien
• Check Point 2200, 4000, 12000, 21400 und 61000 Appliances • Check Point Power-1 • Check Point IP Appliances • Check Point UTM-1 • Check Point IAS
Unterstützte Betriebssysteme
• GAiA • SecurePlatform • IPSO 6.2 Disk-based • Windows
Antivirus Protokolle
• HTTP • HTTPS • FTP • POP3 • SMTP

Identity Awareness Software Blade

ÜBERSICHT

Das Identity Awareness Software Blade ermöglicht einen granularen Blick auf Nutzer, Gruppen und Gerätebasis. Regeln können auf Basis von Identitäten statt auf Basis von IP-Adressen erstellt werden und so den realen Anforderungen an Sicherheitsrichtlinien gerecht werden.

VORTEILE

- Verbesserte Sicht auf Nutzerverhalten
- Vereinfachter Schutz von Unternehmensressourcen
- Einfache Nutzung in jedem Netzwerk

LEISTUNGSMERKMALE

- Frei konfigurierbare Zugriffsrechte
- Nutzung unterschiedlicher Identifikationsmethoden wie Captive Portal und Identity Agent
- Einfache Inbetriebnahme mit Hilfe des „Deployment Wizards“
- Gateway-übergreifende Nutzung möglich

INTERESSANT FÜR

- Unternehmen jeder Größe
- Finanzdienstleister, öffentliche Auftraggeber, Gesundheitswesen und produzierendes Gewerbe
- Unternehmen, die strengen Sicherheitsvorgaben unterliegen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Nahtlose Integration in Active-Directory-Infrastrukturen
- Ermöglicht die Umsetzung granularer Geräte- und userbasierender Regelwerke
- Client-basierende, Portal-basierende oder völlig transparente „Clientless“ User-Identifizierung

GESPRÄCHSEINSTIEG

- Haben Sie Nutzer mit mehreren Endgeräten?
- Arbeiten Ihre Mitarbeiter von verschiedenen Orten aus (Home-Office, vom Kunden, aus dem Büro)?
- Werden bei Ihnen einzelne Rechner von mehreren Personen genutzt?

SPEZIFIKATIONEN

Unterstützte Appliance-Familien	Unterstützte Betriebssysteme
• Check Point 2200, 4000, 12000, 21400 and 61000 Appliances • Check Point Power-1 • Check Point IP Appliances • Check Point UTM-1 • Check Point IAS	• GAiA • SecurePlatform • IPSO 6.2 Disk-based[1] • IPSO 6.2 Flash-based[1] • Windows
Integration in folgende Software Blades	**Identity Agent Unterstützung**
• Firewall • Application Control • DLP • IPS • URL Filtering	• Windows XP Home (SP3, 32-bit) • Windows XP Pro (SP3, 32-bit) • Vista (SP1, 32-bit) • Vista (SP1, 64-bit) • Windows 7 Professional/Enterprise/Ultimate (32-bit) • Windows 7 Professional/Enterprise/Ultimate (64-bit) • Windows Server 2003 (SP1-2, 32-bit) • Windows Server 2008 (SP1-2, 32-bit)

[1]IPSO unterstützt identity enforcement und Logging.

Data Loss Prevention Software Blade

ÜBERSICHT

Check Point revolutioniert den Schutz vor Datenverlusten (Data Loss Prevention, DLP) durch eine Kombination aus Prozessen und Technologien, mit denen Unternehmen den Übergang von der passiven Erkennung hin zu aktiver Verhinderung von Datenverlusten erreichen. Die innovative MultiSpect™-Datenklassifikation kombiniert Benutzer-, Inhalts- und Prozessdaten, um exakte Entscheidungen zu treffen. Zudem versetzt die neue UserCheck™-Technologie Benutzer in die Lage, aufgetretene Datenverluste in Echtzeit zu beheben. Die selbstlernende, netzwerkbasierte DLP-Lösung von Check Point entlastet IT- und Sicherheitsmitarbeiter von der Aufgabe, Vorfälle mit Datenverlust zu bearbeiten. Benutzer erhalten Anweisungen, wie notwendige Richtlinien für die Datenfreigabe umgesetzt werden. Auf diese Weise werden sensible Unternehmensdaten sowohl vor beabsichtigtem als auch vor unabsichtlichem Verlust geschützt.

VORTEILE

- Verhindert den Verlust wichtiger Unternehmensdaten. Neue UserCheck-Technologie ermöglicht Benutzern die Behebung von Datenverlusten in Echtzeit
- Kombiniert Technologien mit Prozessen für ein funktionierendes DLP-System. Die innovative MultiSpect-Datenklassifizierungsengine kombiniert Benutzer-, Inhalts- und Prozessdaten und erreicht so einzigartige Genauigkeit
- Einfache Bereitstellung für eine sofort funktionsfähige Verhinderung von Datenverlusten (DLP). Schützt sensible Daten mittels vorkonfigurierter Richtlinien und umfassender Unterstützung für Dateiformate und Datentypen ab dem ersten Tag

LEISTUNGSMERKMALE

- Wahlweise als integriertes Software Blade oder als Appliance verfügbar
- Schutz ab dem ersten Tag durch vorkonfigurierte Richtlinien
- Offene Skriptsprache bietet anpassbare Flexibilität
- UserCheck™ – Benachrichtigt Benutzer und ermöglicht die selbstständige Problembehebung in Echtzeit
- Schult Benutzer hinsichtlich der Einhaltung der Unternehmensrichtlinien zum sicheren Umgang mit Daten

INTERESSANT FÜR

- Mittelständische und große Unternehmen
- Wichtigste vertikale Märkte: Finanzdienstleistungen, Regierungsbehörden, Gesundheitswesen und Fertigungsindustrie
- Unternehmen, die gesetzliche Vorgaben unbedingt einhalten müssen
- Kunden, die nach Möglichkeiten zum besseren Schutz vertraulicher Daten suchen und gleichzeitig die durch die regulatorische Compliance vorgegebenen Bestimmungen einhalten müssen
- Kunden, welche die Preisgabe von Daten per E-Mail und die teuren Konsequenzen von Geheimnisverlusten befürchten
- Kunden, die eine DLP-Lösung suchen, welche einfach funktioniert und nicht den Geschäftsbetrieb unterbricht oder die IT-Mitarbeiter mit zu vielen False-positive-Ergebnissen oder Warnungen überlastet

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Einfachheit:

- Regelbasierte Richtlinien: Ermöglicht das einfache Festlegen von Sicherheitsrichtlinien, um spezifische Anforderungen zu erfüllen
- Einheitliches Management: Das zentrale Management der gesamten Sicherheitsumgebung sorgt für Transparenz und Kontrolle

Vorbeugung:

- MultiSpect: Identifiziert eine Vielzahl verschiedener, anpassbarer Parameter, die mit spezifischen Sicherheitsvorfällen in Verbindung stehen
- Proaktiv: Verhindert proaktiv absichtlichen und unbeabsichtigten Datenverlust

Innovation:

- UserCheck: Benachrichtigt Benutzer und ermöglicht ihnen die selbstständige Problembehebung in Echtzeit
- Offene Skriptsprache: Erlaubt die Erstellung benutzerdefinierter Datentypen

Flexibilität:

- Bereitstellungsoptionen: Umfasst Inline/Tap, integriert/eigenständig und Appliance/Software/virtualisiert
- Basiert auf der Software-Blade-Architektur. Bietet unerreichte Erweiterbarkeit ohne hohe Zusatzinvestitionen

GESPRÄCHSEINSTIEG

- In welchem Maße stellt Datenverlust ein Problem für Ihr Unternehmen dar?
- Wie viel Zeit und Aufwand benötigen Sie für eine schnelle Implementierung einer DLP-Lösung, d. h. einer Lösung zur Verhinderung von Datenverlusten?
- Wie viel Geld zahlen Sie für professionelle Dienstleistungen im Rahmen der Bereitstellung und der Einrichtung einer DLP-Lösung?
- In welchem Maße beeinträchtigen Einschränkungen durch die Compliance Ihre Geschäftsprozesse?
- Wie verwalten und verfolgen Sie Änderungen an Ihrer DLP-Sicherheitsrichtlinie?
- Wie verhindern Sie, dass Benutzer unbeabsichtigt sensible Daten weitergeben?

Data Loss Prevention Software Blade

SPEZIFIKATIONEN

Das DLP Software Blade ist eine Software-Lösung, die auf der Software-Blade-Architektur basiert. Das DLP Blade kann auf Check Point-Gateways oder Open Servers (siehe Hardware Compatibility List) genutzt werden.

Inspektion		
Inspektionsoptionen	• Über 400 vordefinierte Dateninhaltstypen • Muster, Kennwortabgleich und Wörterbücher • Klassifizierung und Korrelation von Daten mit verschiedenen Parametern • Erweiterte Inspektion auf Grundlage strukturierter Inhalte • Verwendung offener Skriptsprache zur Anpassung und Erstellung eigener Datentypen	
Dateitypen	Inspektion von Inhalten auf Basis von über 800 Dateitypen	
Protokolle	HTTP, HTTPS, SMTP, FTP	
Unterstützte Vorschriften	PCI-DSS, HIPAA, PII und andere	
Nicht regulierte Datentypen	• Daten zu geistigem Eigentum • Finanz- und Rechtsbegriffe • Personalausweisnummern • Bankverbindungen (IBAN) und mehr	
Unterstützung für mehrere Sprachen	Erkennung von Inhalten in mehreren Sprachen, inklusive Single- und Double-Byte-Schriften (UTF-8)	
Enforcement		
Typen	**Fragen des Benutzers** ob eine Nachricht aus der Quarantäne verschickt werden soll **Verhindern:** Verhindert das Senden der Nachricht und informiert Endbenutzer **Erkennen:** Protokolliert Vorfälle und verschickt Nachrichten **Benutzer informieren:** Lässt Übertragung zu, informiert den Benutzer jedoch über mögliche Risiken	
UserCheck	**Pro Regel in mehreren Sprachen anpassbar** **Self-Learning:** Unterbindet eine wiederholte Vorfallverwaltung im gleichen E-Mail-Thread **Zwei Benachrichtigungsmethoden:** E-Mail-Antwort (keine Installation von Agents erforderlich) oder Taskleisten-Popup (setzt Installation eines Thin Agent voraus)	
Enforcement-Funktionen	**Ausnahmen auf Basis von** Benutzern, Benutzergruppen, Netzwerk, Protokoll oder Datentyp **Information des Datenurhebers** bei möglicher Sicherheitsverletzung (z. B. an CFO bei Finanzdokumenten) **Alle Vorfälle protokollieren** mit der Option zur Korrelation von Ereignissen und Prüfung von Vorfällen	
Vorfall anzeigen	Ein Administrator mit DLP-Berechtigungen (und einem dedizierten Kennwort) kann die tatsächliche Nachricht inklusive Anhängen anzeigen. Bei jeder Anzeige einer Nachricht wird ein Prüfprotokoll erstellt. Sie können festlegen, ob Administratoren alle Protokollfelder und die erfassten Daten selbst sehen können oder nicht. Außerdem können die Ansichten des Administrators so gesteuert werden, damit dieser nur bestimmte Vorfallsdaten sehen kann.	
Alle E-Mails prüfen	Bei allen ausgehenden E-Mails (auch ohne Sicherheitsverstoß) werden Absender, Empfänger und Betreff protokolliert.	
Regel-Verwaltung		
Zentrales Management	• Integriert in das SmartCenter Dashboard • Einfache und intuitive Erstellung von Richtlinien • Bequeme Erstellung von Dateninhaltstypen • Effektive Kategorisierung von Dateninhaltstypen und Suchoptionen	
Ereignismanagement	• In SmartEvent integrierte Zusatzfunktionen • Protokollberichte und echtzeitbasierte Überwachung mit Zeitangabe • Kreisdiagramm mit Verteilung der Sicherheitsverletzungen nach Benutzer oder Netzwerk	
Bereitstellung		
Installationsoptionen	• Software Blade, das auf Check Point-Gateways ausgeführt wird • Auf einer dedizierten Appliance (siehe HCL)	
Bereitstellungsoptionen im Netzwerk	Inline-Konnektivität	
Installationsassistent	Wizard zur einfachen Inbetriebnahme des DLP Blades (einschließlich Verbindung zu Active Directory und Konfiguration verschiedener Anfangseinstellungen)	
Minimale Hardware-Anforderungen bei der Installation des DLP Software Blade		
Empfohlene Spezifikationen bei Open Servern	< 1.000 Benutzer	< 5.000 Benutzer
CPU-Kerne	2	8
RAM-Größe	4 GB	4 GB
Speichergröße	250 GB	500 GB
Netzwerkkarten	2	2

Data Loss Prevention

SPEZIFIKATIONEN

Unterstützte Appliance-Familien	Unterstützte Betriebssysteme
• Check Point 2200, 4000, 12000, 21400 und 61000 Appliances • Check Point Power-1 • Check Point IP Appliances • Check Point UTM-1 • Check Point IAS	• GAiA • SecurePlatform

Web Security Software Blade

ÜBERSICHT

Das Check Point Web Security Software Blade bietet umfassenden Schutz vor Angriffen auf die Webinfrastruktur von Unternehmen.

VORTEILE

- Leistungsstarker Schutz vor Buffer-Overflow-Angriffen
- Websicherheit mit Leitungsgeschwindigkeit auf Anwendungsebene
- Unterstützung der Endanwender durch Helpdesk-Webseiten
- Schnelle Bereitstellung
- Kontinuierliche Aktualisierung mit Schutzfunktionen gegen neue Bedrohungen durch Check Point Update Service

LEISTUNGSMERKMALE

- Der Malicious Code Protector arbeitet auf Kernelebene. Dadurch erkennt und blockiert er böswilligen Code im Webdatenverkehr bei voller Leitungsgeschwindigkeit
- Advanced Streaming Inspection verarbeitet den Gesamtkontext der Kommunikation und ergreift ausgehend von den Sitzungs- und Anwendungsdaten geeignete Sicherheitsmaßnahmen. Das entlastet den Kernel und sorgt für eine erhebliche Steigerung des Datendurchsatzes und der Verbindungsraten
- Active Streaming schützt wichtige Site-spezifische Objekte, die von Hackern ausgelesen werden könnten, indem Antwortdaten von Webanwendungen zurückgehalten werden, wenn diese die Serveridentität enthalten. Anschließend wird der Datenstrom entweder verschleiert oder sein Inhalt verändert, um Angreifer zu irritieren
- Einfache Bereitstellung und Verwaltung sowie vollständige Integration des Blade-Managements in die Check Point-Managementoberfläche
- Integration in die Check Point-Berichterstellungs-, Auditing- und Protokollierungsinfrastruktur

INTERESSANT FÜR

- Unternehmen, die bei ihrer Geschäftstätigkeit auf Webanwendungen angewiesen sind
- Unternehmen, die gegenwärtig Webanwendungs-Firewalls evaluieren oder vorhandene Firewalls aktualisieren wollen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Enge Integration in Check Point-Gateways für problemlose Bereitstellung und Verwaltung
- Umfassende und tief greifende Sicherheit für Webanwendungen
- Schutz ohne Signaturen (Zero-Day-Schutz vor Angriffen)
- Durchführung komplexer Inspektionen auf Kernelebene
- Enthält Testmodus zur reinen Überwachung/Testbereitstellung

Web Security Software Blade

GESPRÄCHSEINSTIEG

- Ziehen Sie den Erwerb einer eigenständigen Webanwendungs-Firewall in Betracht? Haben Sie sich aufgrund von Ressourcenbeschränkungen dagegen entschieden?
- Sind Sie mit den Angriffsmethoden gegen Webserver vertraut?

SPEZIFIKATIONEN

Funktion	Beschreibung
Schutzfunktionen gegen Schadcode	Malicious Code Protector (MCP) und allgemeine HTTP-Wurmerkennung
Schutzfunktionen für den Applicationlevel	Cross-Site-Scripting, LDAP-Injektion, SQL-Injektion, Kommando-Injektion und Directory Traversal
Schutzfunktionen gegen Entwendung von Informationen	Schutz vor Header-Spoofing, Schutz vor Verzeichnisauflistung und Verschleierung von Fehlern
Inspektionen des HTTP-Protokolls	Größenbeschränkung des HTTP-Formats, Erzwingung von Nur-ASCII-Anfragen, Erzwingung von Nur-ASCII-Antwortheadern, Definitionen für Header-Injektionen und Definitionen für HTTP-Methoden
Enforcement Optionen	Aktiv, nur überwachen und deaktiviert
Granularität der Konfiguration	Individuelle Server, geschützt durch Web Intelligence Schutzmaßnahmen gegen Angriffe können für jeden Server, für jeden Angriff oder für individuelle Server aktiviert werden, oder es kann sämtlicher HTTP-Datenverkehr überprüft werden. Anpassbare Profile können mit bestimmten Check Point-Gateways verknüpft werden.
Updates	Echtzeit-Updates der Schutzfunktionen und Sicherheitsmaßnahmen durch den Check Point Update Service

Antispam & E-Mail Security Software Blade

ÜBERSICHT

Das Check Point Antispam and Email Security Software Blade bietet umfassenden Schutz für die E-Mail-Infrastruktur von Unternehmen, darunter auch akkuraten Spamschutz und Echtzeitschutz vor einer Vielzahl durch E-Mail verursachter Bedrohungen.

VORTEILE

- Akkurate Erkennung von Bedrohungen in Echtzeit
- Kontinuierliche Aktualisierungen bieten Echtzeitschutz vor Spam und Malware
- Vollständige Kontrolle der Endanwender, ohne dass eine Installation beim Endanwender erforderlich ist
- Schutz vor Phishing und anderen betrügerischen Angriffen durch E-Mail
- Schutz vor Bedrohungen, die von gekaperten Computern aus gesendet werden
- Einfache Konfiguration
- Content- und sprachunabhängig

INTERESSANT FÜR

- Unternehmen jeder Größe, die E-Mail verwenden

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Exakte Spamerkennung
- Schutz vor Angriffen durch Bot-Netze und verseuchte PC
- International einsetzbar dank Inhalts- und Sprachunabhängigkeit
- Vereinfacht durch automatische Updates die laufende Verwaltung

LEISTUNGSMERKMALE

- IP Reputation Antispam überprüft die Reputation des Absenders mit Hilfe einer dynamischen Datenbank bekannter böswilliger IP-Adressen und blockiert so Spam und Malware schon auf Verbindungsebene
- Inhaltsbasiertes Antispam schützt mittels musterbasierter Erkennung vor Spam, der auf Bildern basiert, und Spam in Fremdsprachen
- Mit Hilfe von Negativ- und Positivlisten für Antispam können Administratoren bestimmte E-Mail-Angreifer gezielt blockieren und andere, vertrauenswürdige Absender erlauben.
- Das E-Mail-Antivirenmodul bietet Schutz vor einer Vielzahl von Viren und Malware, darunter auch eingebettete E-Mail-Inhalte und Anhänge
- Der Zero-Hour-Schutz gegen neue Bedrohungen verwendet einzigartige Verteilungsmuster und bietet so Echtzeitschutz vor neuem Spam und neuer Malware
- Der E-Mail-IPS-Schutz schützt vor einer breiten Palette von Angriffen auf die Messaging-Infrastruktur selbst, z. B. Denial-of-Service-Angriffe (DoS) und Buffer-Overflow-Angriffen

GESPRÄCHSEINSTIEG

- Benötigen Sie eine Antispam- und E-Mail-Sicherheitslösung, die kontinuierlich aktualisiert wird, um vor neuen Bedrohungen zu schützen?
- Müssen Sie E-Mail-Sicherheit gewährleisten, aber dabei Ihre IT-Gesamtausgaben reduzieren?
- Setzen Sie gegenwärtig andere Check Point-Sicherheitslösungen ein?
- Müssen Sie das Aufkommen an eingehendem Datenverkehr und den für E-Mail erforderlichen Speicherplatz reduzieren?

SPEZIFIKATIONEN

Funktion	Beschreibung
IP Reputation Antispam	Blockiert Spam und Malware auf Verbindungsebene, indem die Reputation des Absenders mit Hilfe einer dynamischen Datenbank bekannter böswilliger IP-Adressen überprüft wird.
Inhaltsbasiertes Antispam	Schützt mittels musterbasierter Erkennung vor ausgefeilteren Spam-Methoden, darunter auf Bildern basierender und fremdsprachiger Spam.
Negativ- und Positivlisten für Antispam	Nutzt Negativ- und Positivlisten, um offensichtlich böswillige Absender zu blockieren und vertrauenswürdige Absender zuzulassen.
E-Mail-Antivirus	Schützt vor einer Vielzahl von Viren und Malware, inklusive Überprüfung des Inhalts und der Anhänge von Nachrichten
Zero-Hour-Schutz vor neuen Bedrohungen	Schützt mit Hilfe eines umfassenden Analysemoduls proaktiv vor neu aufkommenden Spam- und Malware-Bedrohungen.

Advanced Networking & Clustering Software Blade

ÜBERSICHT

Das Check Point Advanced Networking and Clustering Software Blade erleichtert die Bereitstellung der Netzwerksicherheit sowie der Verwaltung in komplexen, stark ausgelasteten Netzwerken. Zudem optimiert das Blade die Netzwerkleistung und Sicherheit in Multi-Gbits-Umgebungen. Das Advanced Networking and Clustering Software Blade ist ideal für an-spruchsvolle Unternehmens- und Rechenzentrumsumgebungen geeignet, in denen es auf hohe Performance und Verfügbarkeit ankommt.

VORTEILE

- ISP-Redundanz für Zuverlässigkeit und Fehlertoleranz
- QoS-Priorisierung für garantierte Bandbreite und Kontrolle der Latenz
- Application Load Balancing optimiert die Server-Auslastung innerhalb der Stoßzeiten
- SecureXL sorgt für eine umfassende Beschleunigung des Sicherheitsbetriebs
- CoreXL-Multicore-Beschleunigung für einen höheren Deep-Inspection-Durchsatz
- ClusterXL sorgt mit Hochverfügbarkeit und Lastverteilung für maximale Geschäftskontinuität
- Volle Integration in das Check Point Management
- Unterstützung aller Check Point Security Gateways

LEISTUNGSMERKMALE

- Erweitertes Routing
- Multicast-Protokollunterstützung
- QoS-Priorisierung für verschlüsselte und nicht verschlüsselte Daten
- ISP-Redundanz
- Flexible Lastverteilung für Server
- Sicherheitsbeschleunigung mit patentiertem SecureXL
- Multicore-CPU-Unterstützung mit patentiertem CoreXL
- Gateway-Clustering mit patentiertem ClusterXL

INTERESSANT FÜR

- Unternehmen, die erweiterte Netzwerkfunktionen wie Unicast- und Multicast-Routing sowie Routing-Ausstattung für IPv4- und IPv6-Netzwerke benötigen
- Unternehmen, die Echtzeitanwendungen wie VoIP oder Multimedia-Anwendungen einsetzen, welche priorisiert werden müssen
- Unternehmen mit stark ausgelasteten Internet- oder WAN-Verbindungen
- Gateway-Kunden, die eine Mischung aus Skalierbarkeit und Hochverfügbarkeit benötigen
- Gateway-Kunden, die höchste Leistung verlangen, um die steigenden Anforderungen ihrer Kunden erfüllen zu können
- Unternehmen, die ihre Sicherheitsarchitektur erweitern müssen, um mit der sich stets verändernden Bedrohungslage Schritt halten zu können
- ISP und MSSP, die ihre Sicherheitssysteme aktualisieren müssen, um die Sicherheit ihrer Kunden zu gewährleisten

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- QoS-Unterstützung für verschlüsselten und nicht verschlüsselten Datenverkehr über Integration in die Check Point Sicherheits-Gateways
- Flexible Lastverteilung für Server
- QoS-Unterstützung für Fernzugriffsverbindungen Unterstützung für IPv6-Routing auf IP-Appliances
- Zuverlässige, transparente Ausfallsicherung für alle geschäftskritischen Anwendungsverbindungen
- Datendurchsatz mit Leitungsgeschwindigkeit für Gigabit-Netzwerke
- Keine zusätzlichen Load-Balancing-Systeme erforderlich
- Unkomplizierte Bereitstellung und Administration

GESPRÄCHSEINSTIEG

- Setzen Sie gegenwärtig ein Check Point-Security-Gateway oder eine Security-Appliance ein?
- Sind Sie in der Lage, verschlüsselten Datenverkehr auf effiziente Weise zu priorisieren?
- Setzen Sie Echtzeitanwendungen wie VoIP oder Videokonferenzsysteme ein? Durch Sicherheitsuntersuchungen kann die Latenz steigen, daher müssen Echtzeitanwendungen gegenüber anderen Anwendungen bevorzugt behandelt werden.
- Müssen Sie Sicherheits-Gateways und Router in Zweigstellen bereitstellen? Wie sieht es mit verschiedenen Abteilungen in ein und demselben Büro aus?
- Bieten Sie Ihren Kunden garantierte SLAs? Welche Strafen fallen an, wenn Sie SLAs nicht einhalten können?
- Inwiefern sind Sie bei Ihrer alltäglichen Geschäftstätigkeit auf Ihre Hardware angewiesen? Welche Kosten sind mit Hardware-Ausfällen verbunden? Entgangene Umsätze? Kosten für IT-Mitarbeiter? Produktivitätsverluste? Verringerte Kundenzufriedenheit? Betreiben Sie Anwendungen, die Hochverfügbarkeit erfordern, z. B. VoIP, Finanzmarkt-Anwendungen oder PoS-Systeme? Wie sieht Ihre Strategie bei Hardware-Ausfällen aus?
- Haben Sie einen Plan zur Steigerung der Netzwerkleistung?

Advanced Networking Software Blade

SPEZIFIKATIONEN

Das Advanced Networking und Clustering Software Blade, das in viele Check Point-Appliances integriert ist, kombiniert die Funktionen und Vorteile der zwei einzelnen Software Blades: Advanced Networking und Acceleration & Clustering. Diese sind in anderen Appliances weiter verfügbar. In den folgenden Tabellen sind die unterstützten Protokolle und Funktionen sowie Informationen zu den Software Blades aufgeführt, die für die jeweilige Appliance bestellt werden können.

Leistungsmerkmal	Details
Unterstützte Internet-Protokolle	• IPv4 RFC 791 • ICMP RFC 792 • ARP RFC 826 • ICMP Router Discovery (Server) RFC 1256 • Router Discovery v6 (ICMP v6) RFC 24661 • CIDR RFC 1519 • Statisches Routing • Multicast-Tunnel1 • IPv6 Core RFCs1 • VRRPv2 RFC 37681 • VRRPv3 (IPv6) draft-ietf-vrrp-ipv6-spec-08.txt1 • Anforderungen für IPv4 Router RFC 1812 • Quality of Service (QoS)1 • RFC 2474 (allgemeine diffserv-PHB-Informationen) • RFC 3246 (EF-Verhaltensbeschreibung) • RFC 2597 (AF-Verhaltensbeschreibung) • Bootp/DHCP Relay RFCs 951, 2131 • Routing-Aggregation und -Neuverteilung • Nicht nummerierte Schnittstellen • Link Negotiation IEEE 802.3ad • Flow Control IEEE 802.3x • Privates (RFC 1918) und öffentliches IP-Routing • VLAN 802.1Q (transparenter Modus)
Dynamische Routingprotokolle	• RIP RFC 1058 • RIP Version 2 (mit Authentifizierung) RFC 1723 • RIPng (IPv6) RFC 20801 • OSPFv2 RFC 2328 • OSPF NSSA RFC 31011 • OSPFv3 (IPv6) RFC 27401 • BGP4 RFCs 1771, 1963, 1966, 1997, 2918 • BGP4++ RFC 2545, 2858 (Unicast IPv6)
Multicast-Protokolle*	• IGMPv2 RFC 2236 • IGMPv3 RFC 33761 • PIM-SM RFC 4601 • PIM-SSM RFC 46011 • PIM-DM RFC 3973 • PIM-DM state refresh draft-ietf-pim-refresh-02.txt1 • DVMRP (Multicast) RFC 1075[1]
Quality of Service (QoS)	
Minimale Bandbreitenzuweisung	Weighted Fair Queuing (WFQ)-Algorithmus; Garantien können für eine gemeinsame Gruppe von Verbindungen bzw. pro Verbindung eingerichtet werden
Gewichtete Prioritäten	Weist Bandbreite anhand des relativen Nutzens (also der Geschäftsanforderungen) zu
Bandbreitenbeschränkungen	Legt Bedingungenbeschränkungen für nicht kritische Netzwerkanwendungen fest
Low Latency Queuing (LLQ)	Verringert die Latenz bei latenzanfälligem Datenverkehr
Load Balancing für Server	Verteilt Netzwerkverkehr auf verschiedene Server; unterstützt unterschiedliche Lastverteilungsmethoden (inklusive Serverlast, Round Trip, Round Robin, Random und Domäne) sowie Prüfungen der Serververfügbarkeit
Integrierte Differentiated Services (DiffServ)	Ermöglicht Service Providern die Bereitstellung von durchgängigem QoS für VPN- und nicht verschlüsseltem Datenverkehr in IP-WANs
ISP-Redundanz	
Verschiedene Modi	Lastverteilung oder Primär/Backup

* Verfügbar für IP-Appliances

Advanced Networking Software Blade

SPEZIFIKATIONEN

Quality of Service (QoS)	
Produktsupport für SecureXL Firewall (Performance-Pack)[2]	Zugangskontrolle, Verschlüsselung, NAT, Kontoverwaltung und Protokollierung, Verbindungs-/ Sitzungsrate, allgemeine Sicherheitsprüfungen, IPS-Funktionen, CIFs-Ressourcen, Verifizierung von TCP-Sequenzen, dynamisches VPN
Verbindungsvorlagen	Verbindungsbeschleunigung
Trennungsvorlagen	Optimiert Ressourcen
Unterstützte Hochverfügbarkeitsmodi	Aktiv/Passiv und Aktiv/Aktiv
Unterstützte Aktiv/Aktiv-Modi	Multicast und Unicast
Cluster-Protokollport	UDP 8116
Statussynchronisation	Unterstützt ClusterXL- und OPSEC-High Availability (HA)-Lösungen von Drittanbietern
Sticky Decision Function	Sorgt für eine asynchrone Verbindungsunterstützung
WAN-Synchronisation	Wird in Sync-Netzwerken mit einer Latenz von unter 100 ms unterstützt
Duration Limited Synchronization	Hindert Ressourcen daran, Verbindungen von kurzer Dauer zu synchronisieren
Unterstützte Sync-Mitglieder	Bis zu 5 Mitglieder
VLAN-Unterstützung	Ja
Produktsupport für ClusterXL-Firewall2	Authentifizierung/Sicherheitsserver, ACE-Server und SecurID, IPS, Sequenzprüfung, UDP-Kapselung, SAM, ISP-Redundanz, VPN-Peers von Dritten, IP pro Benutzer im Office-Modus
Anti-Spoofing	Verhinderung von Spoofing in internen Netzwerken
ClusterXL-API	Check Point- und ClusterXL-Statusunterstützung von Dritten
Konfiguration wichtiger Geräte	Schnittstellen, Synchronisationsstatus, Status der Firewall-Richtlinie, Prozessstatus von ClusterXL und Firewall
Umfassendes ClusterXL-Management und Status	Bestandteil des Check Point Management

[2] Siehe Versionshinweise und Benutzerhandbuch für weitere Details

APPLIANCE-SUPPORT

Das Advanced Networking und Clustering Software Blade ist in den meisten Check Point-Appliances verfügbar, die 2011 angekündigt wurden. Bei anderen Plattformen werden die Funktionen mit zwei Software Blades bereitgestellt. Die folgende Tabelle enthält Details zur Kompatibilität des Advanced Networking und Clustering Software Blades mit Check Point-Appliances.

SPEZIFIKATIONEN

Appliances	Unterstützte Software Blades
• 12600 • 12400 • 12200 • 4800 • 4600 • 4200 • 2200	• Advanced Networking und Clustering Software Blade
• 61000 • 21400 • Power-1 • IP-Appliances • IAS	• Advanced Networking Software Blade • Acceleration und Clustering Software Blade

Software Blades – Sizing

Mit der nachfolgenden Tabelle finden Sie immer die richtige Größe der einzelnen Blades für Ihr Security Gateway

	Low (S)/DLP 500	Mid (M)/DLP 1500	High End (L)/DLP U	Ultra High End (XL)/ DLP U
Appliances	4600 4400 4200 2200 IP 280 UTM-1 570 UTM-1 270 UTM-1 130 SG80	12200 4800 IP 560 IP 390 IP 290 UTM-1 3070 UTM-1 2070 UTM-1 1070	12400 Power 9070 Power 5070 IP 1280 IP 690	21x00 12600 Power 11000 IP 2450
Software Systeme	SG100 VE801 VE1601	SG400 SG200	SG800 VE4801	SG1200
IAS (Integrated Appliance Solution)		*D1 *D2 *L2 *M2 *R2	*D6 *L6 *M6 *R6	*D8 *L8 *M8 *R8

Check Point
Security Management

Smart-1 Appliances

SmartEvent Appliances

Security Management Software Blades

Multi-Domain Security Management

Smart-1-Appliances

Erweiterbares Sicherheitsmanagement

ÜBERSICHT

Die Smart-1-Serie von Check Point ist eine Produktreihe von Hardware-Appliances, welche die marktführenden Sicherheitsmanagement Software Blades von Check Point mit einer dedizierten Hardware-Plattform kombinieren, die speziell für die Sicherheitsnetzwerke mittelgroßer und großer Unternehmen entworfen wurde. Alle Appliances der Smart-1-Produktreihe basieren auf der Software-Blade-Architektur von Check Point. Sie zeichnen sich durch eine einzigartige Fähigkeit aus, Netzwerksicherheit, IPS und die Endpoint Security Suite in einer einheitlichen Managementlösung zusammenzufassen – und bieten darüber hinaus eine unerreichte Erweiterbarkeit.

Smart-1 150

VORTEILE

- Bietet eine breite Palette von Sicherheitsmanagement Software Blades in Form von vier sofort einsetzbaren Management-Appliances
- Maximiert die Effizienz dank einer einzigen einheitlichen Managementkonsole für Netzwerk- und Endpunktsicherheit
- Senkt Kosten und spart Ressourcen durch die integrierte Speicherkapazität von bis zu 12 TB
- Stellt den kontinuierlichen Geschäftsbetrieb auch in Umgebungen mit höchsten Anforderungen sicher
- Vereinfacht die Umsetzung von Sicherheitsrichtlinien im großen Maßstab mit Multi-Domain-Management (Provider-1)

LEISTUNGSMERKMALE

- Durch die integrierten Managementfunktionen für Netzwerksicherheit, IPS und Endpunktsicherheit können sämtliche Check Point-Produkte zentral verwaltet werden
- Integrierte Fibre-Channel-Unterstützung für SAN und bis zu 12 TB On-Board-RAID-Speicherkapazität für Sicherungen, Wiederherstellung bei Havarien (Disaster Recovery) und die Einhaltung gesetzlicher Vorschriften
- Dank redundanter, Hot-Swap-fähiger Komponenten und integriertem Lights-Out-Management (LOM) können Anwender die Appliance aus der Ferne überwachen und steuern sowie Wartungs- und Administrationsvorgänge am System selbst vornehmen
- Granulare, rollenbasierte Administration mit Multi-Domain-Management (Provider-1), um die einzigartigen Anforderungen großer Unternehmensumgebungen und von Service-Provider-Umgebungen zu erfüllen – einfache Skalierbarkeit bis hin zu Tausenden Nutzern bei gleichzeitiger Senkung der Hardware-Kosten und Optimierung der Betriebseffizienz

INTERESSANT FÜR

- Große Unternehmen mit mehreren Standorten und komplexen Sicherheitsrichtlinien, die ihre Netzwerksysteme austauschen und eine einheitliche Konsole sowie eine einheitliche Oberfläche zur Verwaltung all ihrer Geräte wünschen oder bestrebt sind, ihre Protokolle an einem zentralen Ort zu sammeln, um die Einhaltung gesetzlicher Bestimmungen zu gewährleisten und forensische Analysen zu ermöglichen
- ISP, MSSP, Finanzdienstleistungs-, Produktions- und Kommunikationsunternehmen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Verwaltung der Netzwerkgeräte, IPS und Endpunktsysteme über eine einzige Konsole
- Enthält bis zu 12 TB Hochleistungsspeicher zur Speicherung von Protokollen für die Einhaltung gesetzlicher Vorschriften
- Unterstützt die Archivierung der Protokolle im SAN
- Verbesserte Zuverlässigkeit, Verfügbarkeit und Wartbarkeit dank Hochverfügbarkeit (High Availability, HA), Out-of-Band-Management, Systemstatusanzeige und Hot-Swap-fähiger Komponenten

GESPRÄCHSEINSTIEG

- Versuchen Sie gegenwärtig, Ihre Netzwerkgeräte, IPS und Endpunktsysteme mittels verschiedener Konsolen zu verwalten?
- Machen Sie sich Sorgen um die Einhaltung gesetzlicher Vorschriften?
- Versuchen Sie gegenwärtig, ein komplexes Netzwerk mit verschiedenen Sicherheitsrichtlinien, mehreren geographischen Standorten oder einer Vielzahl von Kunden (MSSP) zu verwalten?
- Machen Sie sich Sorgen über die Datensicherung und die Wiederherstellung bei Havarien (Disaster Recovery)?

Smart-1-Appliances

Erweiterbares Sicherheitsmanagement

HARDWARE-SPEZIFIKATION

Smart-1 Appliances	5	25	50	150
Management HA	Enthalten	Enthalten	Enthalten	Enthalten
Protokolle	7.500	14.000	30.000	30.000
Speicher	1 x 0,5 TB	2 x 1 TB	4 x 1 TB	4 x 1 TB; bis zu 12 TB
Speichertyp	-	RAID 1	RAID 10	RAID 10
Fibre Channel-SAN-Karte	-	-	Optional	Optional
Out-of-Band-Management	-	Integriert	Integriert	Integriert
Gehäuse	1 U	1 U	2 U	3 U
Integrierte Schnittstellen	4 Kupfer-GbE	4 Kupfer-GbE	4 Kupfer-GbE	4 Kupfer-GbE
Abmessungen (Zoll)	17 × 10,9 × 1,75 Zoll	17 × 21,7 × 1,75 Zoll	22,8 × 17,4 × 3,5 Zoll	24,9 × 17,4 × 5,2 Zoll
Abmessungen (metrisch)	431 × 277 × 44 mm	431 × 550 × 44,4 mm	580 × 442 × 88 mm	632 × 442 × 131 mm
Gewicht	6 kg (13,2 lbs)	13 kg (28,7 lbs)	23,5 kg (51,8 lbs)	29,5 kg (65 lbs)
LCD Display	■	■	■	■
Netzteile	1	2	2	3
Netzeingang	100–240 VAC @ 50–60 Hz	100–240 VAC @ 50–60 Hz	90–264 VAC @ 47–63 Hz	90–264 VAC @ 47–63 Hz
DC-Option	-	-	■	-
Spezifikation der Stromversorgung (max.)	150 W	2 x 275 W	2 x 600 W	3 x 930 W
Stromverbrauch (max.)	70,5 W	171 W	505,3 W	399,6 W
Betriebsumgebung	Temperatur: Umgebung 0–40 °C; relative Luftfeuchtigkeit: 5 bis 95 % (nicht kondensierend)			
Compliance	CE, FCC Klasse A, RoHS			
Secure OS	Vorgehärtetes, optimiertes Betriebssystem			
Webbasierte Administration	Schnelle, einfache und sichere Verwaltung von jedem Punkt im Netzwerk			
Backup und Wiederherstellung	Zur Disaster Recovery-Planung			
Zentrale Administratorrechte	RADIUS-Authentifizierung und RADIUS-Gruppen			

SOFTWARE-SPEZIFIKATIONEN

Smart-1-Appliances	5	25	50	150
Verwaltete Gateways	5 bis 25	25 bis 50	50 bis 150	150 bis unbegrenzt
Verwaltete Domänen	1	1	1 bis 3/5/10/50	3 bis 5/10/50
Network Policy Management	■	■	■	■
Endpoint Policy Management	■	■	■	■
Logging und Status	■	■	■	■
SmartProvisioning	■	■	■	■
Monitoring	Optional	■	■	■
User Directory	Optional	■	■	■
SmartEvent Intro	Optional	■	■ *	■ *
Management Portal	Optional	Optional	Optional	Optional
SmartWorkflow	Optional	Optional	Optional	Optional
SmartEvent	Nicht unterstützt	Optional	Optional*	Optional*
SmartReporter	Nicht unterstützt	Optional	Optional*	Optional*
Multi-Domain Security Management (Provider-1)	Nicht unterstützt	Nicht unterstützt	Optional	Optional

* Nicht unterstützt bei Smart-1-Appliances, auf denen Multi-Domain Security Management ausgeführt wird

Smart-1 SmartEvent Appliances

Event-Korrelation als Appliance-Lösung

ÜBERSICHT

Die Smart-1 SmartEvent-Appliances stellen im Rahmen der SmartEvent Software Blades von Check Point Event-Management über eine dedizierte Appliance bereit. Die Lösung wurde für hohe Netzwerksicherheit in mittelständischen und großen Unternehmen entwickelt. Sie analysiert Security-Events in einer sofort einsatzbereiten Plug-and-Play-Appliance. Die Smart-1 SmartEvent-Appliances basieren auf der Software-Blade-Architektur von Check Point. Sie sind die ersten Appliances, die Netzwerksicherheit, IPS und Endpunktsicherheit in einer einheitlichen Managementlösung zusammenfassen und darüber hinaus einzigartige Erweiterungsmöglichkeiten bieten.

VORTEILE

- Einheitliches Ereignismanagement für Netzwerke, Bedrohungen und Endpunktsicherheit
- Bis zu 4 TB integrierter Speicher für Protokoll- und Ereignismanagement
- Hochverfügbarkeit und Redundanz zur Sicherstellung der Betriebskontinuität
- Ereignisanalyse, Korrelation und Berichterstellung für Firewall, IPS, DLP und Endpunkte
- Schnelle Zuordnung kritischer Security-Events mithilfe von Zeitachsen, Diagrammen und Karten
- Einfache Abwehr von Bedrohungen und Angriffen sowie bequemes Hinzufügen neuer Schutzfunktionen
- Schutz vor neuen Bedrohungen mit optionalen Software Blades

LEISTUNGSMERKMALE

- Zentrale Event-Konsole
- Umfassende Transparenz und praxisorientierte Sicherheit
- Integrierte Unterstützung für SANs und bis zu 4 TB On-Board-RAID-Speicherkapazität
- Redundante, Hot-Swap-fähige Komponenten und Lights-Out Management

INTERESSANT FÜR

- Finanzdienstleister, Versorger und staatliche Behörden
- Kunden mit umfangreichen Protokolldaten
- Kunden, die viele Geräte verwalten müssen
- Kunden, die Funktionen für Ereigniskorrelation und Forensik benötigen
- Aktuelle Check Point-Kunden, die folgende Herausforderungen zu bewältigen haben:
  - Mangelnde Informationen über den Gesamtsicherheitsstatus
  - Probleme bei der Ermittlung echter Bedrohungen
  - Schwierigkeiten beim Ergreifen von Maßnahmen und Änderung des Sicherheitsverhaltens auf Grundlage vorhandener Informationen
  - Einhaltung von Audit- und Compliance-Anforderungen

GESPRÄCHSEINSTIEG

- Auf welche Weise analysieren Sie gegenwärtig Ihre Protokolldaten?
- Wie erfüllen Sie interne und externe Audit-Anforderungen?
- Wie priorisieren Sie gegenwärtig Security-Events ?

Smart-1 SmartEvent Appliances

Event-Korrelation als Appliance-Lösung

HARDWARE-SPEZIFIKATION

SmartEvent Appliances	5	25b	50
Verwaltete Gateways	5 bis 25	25 bis 50	50 bis 150
Management HA	Enthalten	Enthalten	Enthalten
Protokollkapazität (empfohlen)	2 GB pro Tag	10 GB pro Tag	25 GB pro Tag
Festplattenspeicher	1 x 0,5 TB	2 x 1 TB	4 x 1 TB
Speichertyp	-	RAID 1	RAID 10
Fibre Channel-SAN-Karte	-	-	Optional
Out-of-Band-Management	-	Integriert	Integriert
Gehäuse	1 U	1 U	2 U
Integrierte Schnittstellen	4 Kupfer-GbE	4 Kupfer-GbE	4 Kupfer-GbE
Abmessungen (Zoll)	17 × 10,9 × 1,75 Zoll	17 × 21,7 × 1,75 Zoll	22,8 × 17,4 × 3,5 Zoll
Abmessungen (metrisch)	431 × 277 × 44 mm	431 × 550 × 44 mm	580 × 442 × 88 mm
Gewicht	6 kg (13,2 lbs)	13 kg (28,7 lbs)	23,5 kg (51,8 lbs)
LCD Display	■	■	■
Netzteile	1	2	2
Netzeingang	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	90–264 VAC, 47–63 Hz
DC-Option	-	-	■
Spezifikation der Stromversorgung (max.)	150 W	2 x 275 W	2 x 600 W
Stromverbrauch (Durchschnitt)	61,7 W	171 W	350,8 W
Betriebsumgebung	Temperatur: Umgebung 0–40 °C; relative Luftfeuchtigkeit: 5 bis 95 % (nicht kondensierend)		
Compliance	CE, FCC Klasse A, RoHS		
Secure OS	Vorgehärtetes, optimiertes Betriebssystem		
Webbasierte Administration	Schnelle, einfache und sichere Verwaltung von jedem Punkt im Netzwerk aus		
Backup und Wiederherstellung	Zur Disaster-Recovery-Planung		
Zentrale Administratorrechte	RADIUS-Authentifizierung und RADIUS-Gruppen		

SOFTWARE-SPEZIFIKATIONEN

SmartEvent Appliances	5	25	50
Verwaltete Gateways	5 bis 25	25 bis 50	50 bis 150
SmartEvent Software Blade	■	■	■
SmartReporter	■	■	■
Logging and Status	■	■	■
Network Policy Management	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Endpoint Policy Management	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
SmartWorkflow	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
SmartProvisioning	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Monitoring	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
User Directory	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
SmartEvent Intro	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Management Portal	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Multi-Domain Security Management	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Network Policy Management Software Blade

ÜBERSICHT

Das Check Point Network Policy Management Blade bietet umfassende Managementfunktionen für Netzwerksicherheitsrichtlinien auf Gateways und Software Blades von Check Point. Den Mittelpunkt der Lösung bildet Smart Dashboard, eine einzige gemeinsame Konsole, mit der auch die komplexesten Bereitstellungsszenarien von Sicherheitsprodukten verwaltet werden können.

VORTEILE

- Optimierte Betriebseffizienz
- Konsistente Durchsetzung von Richtlinien und Kontrolle im gesamten Netzwerk inklusive entfernter Standorte
- Bessere Wahrnehmbarkeit der Sicherheitshaltung im gesamten Unternehmen
- Granulare Kontrolle der Administratorrechte

LEISTUNGSMERKMALE

- Mit den umfassenden Managementfunktionen für Netzwerkrichtlinien können sämtliche Gateways von Check Point konfiguriert und administriert werden
- Die konsistente Durchsetzung von Richtlinien mittels gemeinsamer Geräte- und Netzwerkobjekte ermöglicht die Verteilung ein und derselben Richtlinie im gesamten Netzwerk
- Die intuitive grafische Oberfläche ermöglicht die einfache Verwaltung einer Vielzahl von Sicherheitsrichtlinienfunktionen. Objekte können per Drag-&-Drop-Funktion in Richtlinienfelder eingefügt werden, es können Label und Bereiche für Richtlinien erstellt werden, und es besteht die Möglichkeit, Regeln mit Anmerkungen zu versehen und zwischen den Managementregisterkarten der Software Blades zu navigieren.
- Dank der granularen Kontrolle der Administratorrechte können zu Prüfzwecken oder zur Problembehebung sichere Konten für externe Mitarbeiter und Support-Mitarbeiter erstellt werden, die nur über Lesezugriff oder über Lese-/Schreibzugriff für die Software Blades verfügen

INTERESSANT FÜR

- Kunden, die bereits Gateways von Check Point einsetzen und auf der Suche nach erweiterten Managementfunktionen sind

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Verwaltung sämtlicher Check Point-Produkte über eine einzige Konsole
- Integrierte, intuitive grafische Oberfläche
- Granulare Kontrolle der Administratorrechte

GESPRÄCHSEINSTIEG

- Würden Sie gern alle Ihre Check Point-Produkte über eine einzige Konsole konfigurieren?
- Würde die Verwaltung über eine einzige Konsole eine Senkung Ihrer Betriebskosten bewirken?
- Würde zentrale Verwaltung Ihre Sicherheit verbessern?
- Wäre rollenbasierte Administration mit klaren Kompetenzen und Zuständigkeiten von Vorteil für Ihr Unternehmen?

Network Policy Management Software Blade

SPEZIFIKATIONEN

Funktion	Beschreibung
Unified Security Gateway Software Blade-Management	Firewall, VPN, IPS, Web Security, URL Filtering, Antivirus & Anti-Malware, Antispam & Email Security, Advanced Networking, Acceleration & Clustering und Voice over IP
Suche	Fragt Objekte und die Regelbasis ab
Management von Regeln	Unterteilung in Abschnitte und Label
Versionen	Ermöglicht die Erstellung und Verwaltung mehrerer Richtlinienversionen — automatisch oder manuell
Sicherung und Wiederherstellung	Erstellt problemlos exakte Kopien von Network Policy Management Software Blades zur Wiederherstellung im Schadensfall
Hochverfügbarkeit	Unterstützt die Konfiguration von Standby-Network Management Policy Software Blades
Rollenbasierte Administration	Globale(r) und granulare(r) Administrationszugriff und -berechtigungen
Multi-Plattform-Unterstützung	Windows Server, Red Hat Linux, Solaris, IPSO und SecurePlatform
Revisionskontrolle	Aufbewahrung verschiedener Richtlinienversionen
Authentifizierung	LDAP, RADIUS, TACACS, TACACS+, SecurID und lokale Datenbank
Intuitives Policy Management	Ziehen und Ablegen, Aufteilung der Software Blades auf verschiedene Registerkarten
OPSEC API	Integration mit Produkten von Drittanbietern
SNMP	Check Point-MIB bei IANA registriert

Endpoint Policy Management Software Blade

ÜBERSICHT

Mit dem Endpoint Policy Management Software Blade können Sie von einer einzigen Konsole aus zentral Sicherheitsrichtlinien für alle Endgeräte im Unternehmen bereitstellen, verwalten, überwachen und durchsetzen, und zwar in Unternehmen jeder Größe.

VORTEILE

- Zentralisiert und delegiert Managementoptionen
- Zentrale Überwachung und Berichterstellung für alle Kontrollstellen für Endpunktsicherheit
- Schnellere Entdeckung, Überwachung und forensische Analyse von Sicherheitsvorfällen
- Umfassende Berichtsfunktionen und Unterstützung für Audits und Compliance
- Nutzt einen einzigen Agenten und ermöglicht so die schnellere, einfachere Bereitstellung ohne manuellen Eingriff der IT-Mitarbeiter oder der Endanwender vor Ort
- Einheitliche Endpunktsicherheit mit Verwaltung von Sicherheitsereignissen im Netzwerk

LEISTUNGSMERKMALE

- Die Firewall-Regeln bieten die gleiche Schutzstufe wie die Perimeter-Firewall, um Netzwerkaktivitäten ausgehend von den Verbindungsinformationen einschränken oder erlauben zu können
- Dank Zugriffszonen und Zonenregeln können Standortgruppen erstellt werden, über die Netzwerkzugriffsrechte zugewiesen werden
- Richtlinien zur Anwendungskontrolle schränken den Netzwerkzugriff aus Anwendungsbasis ein
- Dank Program-Advisor-Service-Richtlinien erfolgt das Management der Anwendungskontrolle automatisch
- Anwendungsrichtlinien stellen sicher, dass jeder Endpunkt alle Anforderungen bezüglich der Anwendungen erfüllt und über die geforderten Versionen verfügt, bevor der Zugriff auf das Netzwerk gestattet wird
- Anwender, die die Anforderungen nicht erfüllen, werden durch Cooperative-Enforcement®-Richtlinien auf Netzwerkzugriffsebene bzw. Authentifizierungsebene eingeschränkt oder vom Netzwerk getrennt
- Die Anti-Spyware-Richtlinien von Check Point erkennen und entfernen Spyware, um die Unternehmensdaten zu schützen
- Die Antivirus-Richtlinien von Check Point bieten zentral verwalteten Antivirenschutz für Endpunkte

INTERESSANT FÜR

- Unternehmen, die Endpunktsicherheit auf einer Vielzahl von Endpunkten bereitstellen müssen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Granulare, skalierbare und intuitive grafische Oberfläche
- Rollenbasierte Zugriffsregeln
- Fasst alle wichtigen Sicherheitsfunktionen in einer einzigen Managementkonsole zusammen: VPN, Firewall, NAC, Browser, Antivirenschutz, Anti-Sypware-Schutz und Anwendungskontrolle

GESPRÄCHSEINSTIEG

- Sind Sie auf der Suche nach einer intuitiven und gleichzeitig granularen Oberfläche für die Endpunktverwaltung?
- Hätten Sie gern eine einzige Managementkonsole, mit der Sie VPN, Firewall, NAC, Browser, Antivirenschutz, Anti-Spyware und Anwendungen bereitstellen und konfigurieren können?

Endpoint Policy Management Software Blade

SPEZIFIKATIONEN ENDPOINT SECURITY CLIENT

Plattform	Betriebssystem
Windows	• Windows XP SP3 und höher • Windows Vista 32/64 Bit • Windows 7 (32/64 Bit) • Windows Server 2008/2008 R2 (32/64 Bit) – Malwareschutz/Firewall/Compliance

ENDPOINT SECURITY MANAGEMENT

Security Management Server OS	Version
Windows	• Microsoft Windows Server 2003 32/64 Bit • Microsoft Windows Server 2008/2008 R2 32/64 Bit
SmartConsole OS	**Version**
Windows	• Windows XP SP3 und höher • Windows 7 (32/64 Bit) • Windows 2003 Server

HARDWARE FÜR ENDPOINT SECURITY MANAGEMENT

Hardware	Mindestanforderungen
CPU	Intel Pentium-Prozessor E2140 oder äquivalenter Prozessor mit 2 GHz
Speicher	2 GB
Datenträger	4 GB
Netzwerk	LAN

Neu in E80.40:

- Nutzung des EPM Blades auf dem existierenden Smart Center
- Ein dediziertes Management ist damit nicht mehr nötig, jedoch weiterhin möglich

Logging & Status Software Blade

ÜBERSICHT

Ab der Version 75.40 profitieren Sie außerdem von SmartLog als Bestandteil des Logging und Status Blades, womit Sie weitere Vorteile nutzen können: Das Check Point Logging & Status Software Blade stellt mittels Protokollen umfassende Informationen zu Sicherheitsaktivitäten zur Verfügung und bietet einen vollständigen visuellen Überblick über Änderungen an Gateways, Tunnel, Remote-Benutzer und Sicherheitsaktivitäten. Ab der Version 75.40 profitieren Sie außerdem von SmartLog als Bestandteil des Logging und Status Blades, womit Sie weitere Vorteile nutzen können: Check Point SmartLog wandelt Daten durch sekundenschnelle Suchvorgänge, die für unmittelbare Transparenz sorgen, in Sicherheitsdaten um. Hierzu steht eine einfache, intuitive und Google-ähnliche Suchoberfläche zur Verfügung. Außerdem lassen sich mit der zentralen Sicherheitsmanagement-Konsole von Check Point Milliarden Protokolldatensätze für verschiedene Zeiträume und Domänen erzeugen.

VORTEILE

- Reduziert die zur Behebung von Konfigurationsfehlern benötigte Zeit und die Administratoraktivität, indem alle protokollierten Verbindungen in Echtzeit grafisch verfolgt werden
- Identifiziert wichtige Aktivitäten mittels vordefinierter Protokollabfragen für die verschiedenen Produkte
- Einfache Verwaltung des Datenvolumens durch automatische Protokollpflege
- Enge Integration mit Berichterstellungslösungen von Drittanbietern über die OPSEC LEA API
- Sichere Verwaltung sensibler Daten
- Suchergebnisse in Sekundenbruchteilen für beliebige Protokollfelder
- Detaillierte Suche nach Kommunikations- oder Datenverkehrsmustern
- Schnelle und verständliche Statistiken
- Für große Umgebungen geeignet
- Schnelle Fehlerbehebung dank echtzeitbasierter Meldungen
- Keine lizenzseitige Protokollbegrenzung (Begrenzung ausschließlich durch Festplattengröße)

LEISTUNGSMERKMALE

- Die Darstellung und Fehlerbehebung in Echtzeit ermöglicht die visuelle Verfolgung aller protokollierter Verbindungen und Administratoraktivitäten und reduziert auf diese Weise deutlich die Zeit, die zur Behebung von Fehlern benötigt wird
- Dank der flexiblen Bereitstellungsoptionen hat der Administrator vollständige Kontrolle über sensible Daten und kann z. B. den Speicherort der Protokolle festlegen sowie die Systeme so auslegen, dass sie mit den Anforderungen des Unternehmens an die Protokollkapazität übereinstimmen
- Bei Erreichen des konfigurierbaren Größenlimits werden die Protokolle automatisch ausgetauscht. Dadurch haben Administratoren volle Kontrolle über die ausgetauschten Protokolldateien und können sicherstellen, dass der verfügbare Festplattenspeicher nicht überschritten wird
- Enge Integration mit Berichterstellungslösungen von Drittanbietern über die sichere OPSEC LEA API
- SmartLog – die Protokoll-Analyse der nächsten Generation
- Einfache, intuitive und Google-ähnliche Suchoberfläche
- Transparenz und Fehlerbehebung in Echtzeit
- Einfache Bereitstellung
- Leistungsfähige und einfache Abfragen
- Umfassende Integration in das Management von Check Point

INTERESSANT FÜR

- Alle Check Point-Kunden, die umfangreiche Protokolle generieren und diese aus rechtlichen Gründen und aus Gründen der Compliance aufbewahren müssen
- Alle Kunden, die Protokolle erfassen, analysieren, verwalten und archivieren müssen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Vollständiger visueller Überblick über die Sicherheitsaktivitäten
- Einfache Analyse von Datenverkehrsmustern und Sicherheitsproblemen
- Ermöglicht Administratoren die schnelle Erfassung von Daten aus rechtlichen Gründen oder zu Audit-Zwecken
- Enthält vordefinierte und anpassbare Protokollabfragen
- Automatische Archivierung der Protokolle beim Erreichen der Grenzwerte für den Speicherplatz
- Suche in verschiedenen Protokolldateien, Zeiträumen, Gateways und Domänen
- Möglichkeit zur zentralen Protokollsuche in Umgebungen mit mehreren Domänen
- Suchergebnisse in Sekundenbruchteilen für beliebige Protokollfelder: Anzeige der ersten 50 Ergebnisse nach 655 ms aus 374.727.254 Protokollen; Suche in über 3 Millionen Protokollen in weniger als einer Sekunde
- SmartLog ist in jedes R75.40 Logging and Status Software Blade integriert
- Zentrales Tracking von Sicherheitsaktivitäten in allen Software Blades über eine zentrale Konsole

Logging & Status Software Blade

GESPRÄCHSEINSTIEG

- Wie verfahren Sie mit den umfangreichen Protokollen, die von Firewalls, Endpunkten und Enforcement Points generiert werden?
- Müssen Sie bei der Verwaltung von Protokollen interne oder gesetzliche Auditing-Anforderungen beachten?
- Überprüfen Sie Ihre Protokolle manuell?
- Welche verdächtigen Verhaltensmuster verfolgen Sie?
- Wie oft überprüfen Sie Ihre Protokolldatensätze?
- Wie lange brauchen Sie, um bestimmte Protokolldatensätze zu finden?
- Haben Sie die Möglichkeit, Protokolldatensätze aller Regionen, Server und Domänen zu verfolgen?

SPEZIFIKATIONEN

Funktion	Beschreibung
Protokollformat	Wie in der OPSEC LEA API definiert
Packet Capture	Verfügbar für IPS-Ereignisse
Protokolltypen	Verbindung, aktiv, Audit und weitere (je nach Produkt)
Arten von Ereignisbenachrichtigungen	Protokoll, Alarm, SNMP-Trap, E-Mail und benutzerdefiniertes Skript
Granulare Protokollierungsoptionen	Globale Sicherheitsrichtlinien-Regelbasis für implizite Regeln und weitere Optionen
Sichere Protokollübermittlung	Über Check Point Secure Internal Infrastructure
Automatischer Wechsel von Protokolldateien	Bis zu 2 GB (Standardwert), konfigurierbar
Wechsel der Protokolldatei	Manuell oder automatisch, zu einer bestimmten Zeit oder bei einer bestimmten Größe der Protokolldatei
Pflege der Protokolldatei	Bei der Protokollierung kann ein prozentualer Anteil des Festplattenspeichers frei gehalten werden, die Protokolle können für einen bestimmten Zeitraum aufbewahrt werden, und es können benutzerdefinierte Skripte ausgeführt werden.
Backup-Protokollserver	Die Protokolle können lokal gespeichert oder an alternative Protokollserver gesendet werden.
Vordefinierte und anpassbare Protokollanfragen	Vordefiniert je nach Produkt
Anpassbare Protokollfilter	Nach Protokollfeld
Remote-Management von Protokolldateien	Wechsel, Ansicht und Abruf über Tracker
Standardtools und benutzerdefinierte Tools	Ping, whois und nslookup
An SmartMap angedockte und nicht angedockte Ansicht	Nicht angedockte Ansicht für bessere Lesbarkeit der Karte
SmartMap-Layouts	Hierarchisch (Baum) oder symmetrisch
Enge SmartMap-Integration	Erstellen, Bearbeiten und Löschen von Objekten sowie Anzeige, wo diese gerade verwendet werden
SmartMap-Exporte	Visio- oder Bilddatei
SmartMap Navigator	Unterstützt die Anzeige komplexer Topologien

HARDWARE FÜR ENDPOINT SECURITY MANAGEMENT

	Smart-1 5	Smart-1 25	Smart-1 50
Verwaltete Gateways	5–25	25–50	50–150
Gerätespeicher	500 GB	2 x 1 TB	4 x 1 TB
Tägliche Protokollkapazität ohne SmartLog	2 GB	12 GB	25 GB
Tägliche Protokollkapazität mit SmartLog	3,6 GB	21,6 GB	45 GB
Aufbewahrungszeitraum von SmartLog*	1 Monat	1 Monat	1 Monat

* Die Speicherzeiten für Protokolle werden anhand des verfügbaren Speichers im Gerät berechnet und umfassen sowohl Protokolle als auch den SmartLog-Indexspeicher.

SmartWorkflow Software Blade

ÜBERSICHT

Das Check Point SmartWorkflow Software Blade stellt einen formalen Prozess für das Änderungsmanagement be Sicherheitsrichtlinien zur Verfügung, mit dem Administratoren die Fehlerhäufigkeit reduzieren und die Einhaltung der Vorschriften verbessern können. Es automatisiert das Änderungsmanagement bei Richtlinien und bietet visue Verfolgbarkeit und vollständige Audit-Möglichkeiten.

VORTEILE

- Etabliert einen formalen Prozess für die Verfolgung, Genehmigung und die Überprüfung von Änderungen an der Sicherheitsrichtlinie
- Vereinfacht das Änderungsmanagement und steigert die Betriebseffizienz
- Reduziert die Fehlerhäufigkeit durch granulare Sichtbarkeit von Richtlinienänderungen
- Fügt sich nahtlos in den bereits vorhandenen Genehmigungsprozess des Änderungsmanagements ein
- Vereinfacht die Einhaltung von Vorschriften durch Audit-Trails und integrierte Rollenteilung
- Bietet vollständiges Lebenszyklusmanagement für Richtlinien aus einer Hand

LEISTUNGSMERKMALE

- Das automatische Änderungsmanagement versetzt Administratoren in die Lage, die Änderungen an Regelbasen, Netzwerkobjekten, Sicherheitsrichtlinien, Benutzern, Administratoren, Gruppen, OPSEC-Anwendungen, VPN-Gemeinschaften und Servern zu verfolgen
- Einfache Visualisierung der Änderungen, wobei sämtliche Änderungen an Regeln und Objekten in SmartDashboard und in Sammelberichten über Änderungen hervorgehoben werden
- Falls im Unternehmen bereits Genehmigungsprozesse des Änderungsmanagements etabliert wurden, kann die Sitzungsgenehmigung daran angepasst werden. Dabei werden sowohl Manager- als auch Administratorgenehmigungen sowie Installationsrichtlinien für Notfälle unterstützt
- Mittels Richtlinienrevisionen und der Grundlagenvergleichsfunktion können Manager den Sammelbericht über Änderungen überprüfen, der Informationen zu hinzugefügten, geänderten und entfernten Objekten enthält, und diese Änderungen anschließend mit der aktuellen Sicherheitsrichtlinie vergleichen
- Mit Hilfe von Audit-Trails können Administratoren Änderungen an Objekten und Sicherheitsrichtlinien sowie Sitzungsereignisse über lange Zeiträume hinweg verfolgen

INTERESSANT FÜR

- Große Kunden, die häufig Richtlinienänderungen vornehmen
- Kleine und mittelgroße Kunden, die noch nicht über einen formalen Prozess für das Änderungsmanagement verfügen
- Höhere Leitungsebenen des Unternehmens (Director/Manager IT oder höher), da manche IT-Administratoren den formalen Prozess für das Änderungsmanagement, wie er von SmartWorkflow erzwungen wird, unter Umständen als Einschränkung ihrer Freiheit betrachten

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Erleichtert leitenden Mitarbeitern die formale Verfolgung, Genehmigung und Überprüfung von Änderungen an der Sicherheitsrichtlinie
- Bietet die Möglichkeit zur Aufhebung der Richtlinien im Notfall, wobei Audit-Trails erstellt werden
- Kann an bereits vorhandene Autorisierungsprozesse angepasst werden
- Ermöglicht bei Bedarf die Rücknahme von Änderungen

GESPRÄCHSEINSTIEG

- Nehmen Sie häufig Änderungen an Ihren Sicherheitsrichtlinien vor? Machen Sie sich Sorgen darum, dass Änderungen Sicherheitsrisiken mit sich bringen könnten?
- Verfügen Sie über einen formalen Prozess für das Änderungsmanagement?
- Wie erfahren Sie davon, dass eine Richtlinie geändert wurde?

SmartWorkflow Software Blade

SPEZIFIKATIONEN

Funktion	Beschreibung
Session-basierte Richtlinienänderungen	• Änderungen an Sicherheitsrichtlinien werden im Kontext von Sessions durchgeführt. • Zur Klarstellung können den Sessions Hinweise hinzugefügt werden. • Änderungen, die innerhalb einer Session durchgeführt wurden, können verworfen werden. • Sessions, die zur Genehmigung übermittelt wurden, sind zur Bearbeitung gesperrt.
Flexible Autorisierung	• Rollenbasierte Genehmigung (Vier-Augen-Prinzip) • Eigengenehmigung • Notfall-Bypass (erfordert Kennwort)
Richtlinieninstallation	• Es können nur genehmigte Richtlinien installiert werden. • E-Mail-Benachrichtigung über Installation
Hervorhebung	• Änderungen werden in SmartDashboard hervorgehoben. • Liste der Änderungen in SmartDashboard
Berichte	• Bietet Berichte zu Session-Änderungen im HTML-Format. • Die Berichte können gespeichert, gedruckt und per E-Mail versendet werden.
Verfolgung von Session-Informationen	• Der Abschnitt „Session-Informationen“ enthält Informationen zur Session, Anmerkungen sowie eine Liste der Änderungen. • Ermöglicht die sequenzielle Überprüfung von Änderungen.
Session-Verfolgung	• Anzeige aller erstellten Sessions • Anzeige der Sessions-Änderungen • Anzeige des Sessionstatus (ausstehend, genehmigt, abgelehnt usw.)
Vergleich von Sessions	• Vergleich von Änderungen zwischen verschiedenen Sessions • Vergleich der Änderungen zwischen einer installierten Session und einer genehmigten Session
Umfassendes Auditing	• Jeder Schritt einer Session wird protokolliert (Erstellung der Session, Einreichung, Genehmigung/Ablehnung und Installation). • Für jede in einer Session vorgenommene Änderung wird ein Eintrag im Audio-Protokoll erstellt. • Alle Audit-Protokolle von Sessions verfügen über eine Session-Nummer, um die Filterung zu ermöglichen. • Alle Audit-Protokolle von Sessions enthalten eine Beschreibung der Änderungen (alter/neuer Wert) sowie Session- und Administrationsinformationen. • Die Audit-Protokolle der Session werden an SmartView Tracker übermittelt. • Bei jeder Änderung an Objekten oder Richtlinien wird ein Eintrag im Audit-Protokoll erstellt.
Check Point Management-Integration	• Nahtlose Integration mit Check Point Network Policy Management • Check Point Multi-Domain Security Management (Provider-1) Unterstützung • Verfolgung von Änderung an CMAs • Verfolgung von Änderungen der globalen Richtlinie

Monitoring Software Blade

ÜBERSICHT

Das Check Point Monitoring Software Blade überwacht zentral Check Point- und OPSEC-Systeme und liefert ein vollständiges Bild über Änderungen an Gateways, Tunneln, Remote-Benutzern und Sicherheitsaktivitäten.

VORTEILE

- Hält die hohe Verfügbarkeit des Netzwerks aufrecht
- Verbessert die Effizienz der Bandbreitenausnutzung
- Verfolgt die Einhaltung von SLAs
- Steigert den ROI im Sicherheitsbereich
- Reagiert schnell auf Netzwerk- und Sicherheitsänderungen

LEISTUNGSMERKMALE

- Mit Hilfe der Gateway-Überwachung können Administratoren die Systemdaten, die Netzwerkaktivität, den Richtlinien- und den Lizenzstatus sowie weitere Gateway-spezifische Daten anzeigen
- Zur Überwachung des Netzwerkverkehrs stehen Graphen und Diagramme in Übersichtsform sowie in detaillierter Form zur Verfügung. Mittels dieser Graphen und Diagramme können Muster im Netzwerkverkehr analysiert, die Netzwerknutzung überprüft und Kostenschätzungen erstellt werden.
- Die Funktion zur Überwachung verdächtiger Aktivitäten kann die Zugriffsrechte anpassen, wenn verdächtige Aktivitäten festgestellt werden. Zusätzlich kann sie so konfiguriert werden, dass Administratoren beim Eintreten vordefinierter Systemereignisse automatisch benachrichtigt werden.
- Die Überwachungsfunktion für VPN-Tunnel überwacht das ordnungsgemäße Funktionieren der Tunnelfunktionen. Dadurch können Fehlfunktionen und Konnektivitätsprobleme schnell behoben werden.
- Die Überwachungsfunktion für Remote-Benutzer stellt umfassende Informationen über geöffnete Remote-Sitzungen, überlappende Sitzungen, Routing-Datenverkehr und Verbindungszeiten zur Verfügung, so dass Probleme mit der Remote-Konnektivität identifiziert und behoben werden können
- Die Überwachungsfunktion für Cooperative Enforcement überprüft eingehende Verbindungen, die von internen Hosts und entfernten Hosts ausgehen, und protokolliert autorisierte und nicht autorisierte Hosts
- Mit Hilfe der grafischen Berichtsfunktion können Administratoren den Datenverkehr auf einzelnen Gateways oder in einzelnen Segmenten analysieren und so mögliche Ursachen für die Beeinträchtigung der Netzwerkleistung identifizieren
- Enge Integration mit anderen Check Point-Produkten

INTERESSANT FÜR

- Kunden, die bereits Gateways von Check Point einsetzen und auf der Suche nach erweiterten Management-, Überwachungs-, Benachrichtigungs- und Berichterstellungsfunktionen sind

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Umfassende Überwachung aller Check Point- und OPSEC-Netzwerkelemente und des jeweiligen Datenverkehrs
- Eine einheitliche Konsole mit vordefinierten und anpassbaren Oberflächen
- Enge Integration mit der Check Point-Managementarchitektur

GESPRÄCHSEINSTIEG

- Müssen Sie die Netzwerkleistung und die Leistung Ihrer Sicherheitssysteme überwachen?
- Sind Sie darauf angewiesen, Anomalien im Datenverkehr und Sicherheitsbedrohungen schnell erkennen zu können?
- Müssen Sie analysieren, welche Faktoren unter Umständen die Netzwerkleistung beeinträchtigen?

Monitoring Software Blade

SPEZIFIKATIONEN

Funktion	Beschreibung
Sichere Status-Updates von Remote-Modulen	Über Check Point OPSEC APIs wie AMON
Anpassbare Systemübersicht	Inklusive: • Anpassung nach Gateway • Gesamtstatus • Durchschnittliche Prozessorbelastung • Arbeitsspeicher • Freier Festplattenspeicher (%)
Systeminformationen	Betriebssystem, Prozessor, Arbeitsspeicher, freier Festplattenspeicher (%) und Netzwerkaktivitäten
Statusinformationen zum Produkt	Inklusive: • Firewall • VPN • ClusterXL • Antivirus
Anpassbare Schwellwerteinstellungen	Es können globale Aktionen oder Aktionen für einzelne Gateways festgelegt werden, die beim Erreichen eines Schwellwertes ausgeführt werden (z. B. beim Ausfall eines Remote-Gateways).
Anpassbare Aktionen	Protokoll, Alarm, E-Mail, SNMP-Trap und benutzerdefiniert
Anpassbares Reporting	Gateways, Datenverkehr, Zähler, Tunnel und Remote-Benutzer
Rücksetzung von Benutzern und Tunneln	Kontrolliert die Benutzeraktivitäten
Anwendung einer dynamischen Erzwingungsrichtlinie	Pro Gateway, Quelle, Ziel und Dienst
ClusterXL Member Control	Start und stoppt die ClusterXL-Prozesse.

Management Portal Software Blade

ÜBERSICHT

Das Check Point Management Portal Software Blade ermöglicht Browser-basierten Managementzugriff für Außenstehende wie Mitarbeiter des technischen Supports oder Prüfer, während gleichzeitig die zentrale Kontrolle der Durchsetzung von Richtlinien aufrechterhalten wird. Anwender vom Managementportal können die Sicherheitsrichtlinien, den Status aller Check Point-Produkte und die Administratoraktivitäten anzeigen. Zusätzlich können sie interne Benutzer erstellen und bearbeiten.

VORTEILE

- Vereinfacht das Management der Sicherheitskonfiguration und die Fehlerbehebung
- Erweiterter Zugriff auf die Einstellungen der Netzwerkrichtlinie für externe Prüfer
- Begrenzt zuverlässig die Offenlegung der Sicherheitsmanagementfunktionen

LEISTUNGSMERKMALE

- Ausgewählte Personen erhalten Lesezugriff auf eine Ansicht der Netzwerkrichtlinie und -objekte, ohne dass die zentrale Kontrolle über die Durchsetzung der Richtlinie aufgegeben wird
- Prüfer, Mitarbeiter des technischen Supports und andere autorisierte Gruppen erhalten einen sicheren Fernzugriff über SSL und können die Netzwerkrichtlinie und die Netzwerkobjekte, die IPS-Einstellungen und die Statusinformationen der Gateways betrachten
- Mit Hilfe der komfortablen Benutzeroberfläche kann problemlos Zugriff auf den Gateway-Status gewährt werden, und es kann eine Vielzahl von Problembehebungsmaßnahmen aus der Ferne durchgeführt werden

INTERESSANT FÜR

- Managed Security Service Provider (MSSP), die ihren Kunden Sicherheits- bzw. Netzwerkkonfigurationsdaten zur Verfügung stellen müssen
- Unternehmen, die Sicherheits- bzw. Netzwerkkonfigurationsdaten an Zweigstellen oder Prüfer übermitteln müssen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Remote-Überwachung der Netzwerk- bzw. Sicherheitskonfiguration
- Ermöglicht die Zusammenarbeit per Fernzugriff, um Gegenmaßnahmen gegen Angriffe einzuleiten und Fehler im Netzwerk zu beheben
- Ermöglicht MSSP die sichere, gemeinsame Nutzung von Konfigurations- und Protokolldaten mit Kunden

GESPRÄCHSEINSTIEG

- Sind Sie ein MSSP? Müssen Sie auf sicherem Wege Richtlinien, Objekte, IPS-Einstellungen oder den Gateway-Status an Ihre Kunden übermitteln?
- Sind Sie ein großes Unternehmen? Müssen Sie auf sicherem Wege Richtlinien, Objekte, IPS-Einstellungen oder den Gateway-Status an Zweigstellen übermitteln?
- Sind Sie ein mittelgroßes Unternehmen? Müssen Sie auf sicherem Wege Richtlinien, Objekte, IPS-Einstellungen oder den Gateway-Status an Remote-Prüfer und technische Mitarbeiter übermitteln?

SPEZIFIKATIONEN

Funktion	Beschreibung
SSL-Zugang	Unterstützt
Konfigurierbare Ports	Unterstützt
Konfigurierbare Rollen	Berechtigung für spezifische Managementportale
Lese-/Schreibzugriff	Hinzufügen von Benutzern und Management von Protokollen
IP-Zugriffskontrolle	Beschränkt den Zugriff auf bestimmte IP-Adressen

User Directory Software Blade

ÜBERSICHT

Das Check Point User Directory Software Blade nutzt LDAP-Server, um Authentifizierungs- und Sicherheitsinformationen über Netzwerkbenutzer abzurufen, und ermöglicht so eine zentrale Benutzerverwaltung für das gesamte Unternehmen.

VORTEILE

- Ermöglicht Sicherheits-Gateways von Check Point den Abruf von Benutzerauthentifizierungs- und Sicherheitsinformationen
- Integriertes, erweitertes LDAP-Schema enthält sämtliche für die Benutzersicherheit erforderlichen Elemente
- Ermöglicht die zentrale Benutzerverwaltung im gesamten Unternehmen, indem die Sicherheitsrichtlinie des Unternehmens bei allen LDAP-kompatiblen Anwendungen durchgesetzt wird

LEISTUNGSMERKMALE

- Beseitigung von Risiken, die mit der manuellen Pflege und Synchronisierung redundanter Daten verbunden sind, indem LDAP-basierte Speicher für die Benutzerdaten verwendet werden
- Unterstützung für Microsoft Active Directory und andere führende LDAP-Lösungen
- Verwaltung des LDAP-Verzeichnisses über SmartDashboard

GESPRÄCHSEINSTIEG

- Würden Sie gern Ihre Active-Directory-Datenbank für Ihre Check Point-Sicherheitsrichtlinien verwenden?
- Wünschen Sie sich eine leicht bedienbare grafische Oberfläche zur Bearbeitung von LDAP-Objekten?

INTERESSANT FÜR

- Check Point-Kunden mit drei oder mehr Gateways
- Finanzdienstleistungsunternehmen, Bildungseinrichtungen, Gesundheitswesen, Produktionseinrichtungen und Managed Security Service Provider

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Zentraler Datenspeicher reduziert den Verwaltungsaufwand und verhindert Fehlkonfigurationen
- Kompatibel mit verschiedenen LDAP-Anbietern
- Unterstützt LDAP und LDAP over SSL (LDAPS)
- Bietet eine komfortable grafische Oberfläche, mittels derer Administratoren Benutzer, Gruppen und andere Objekte anzeigen, bearbeiten und erstellen können

SPEZIFIKATIONEN

Funktion	Beschreibung
Unterstützte LDAP-Anbieter	Microsoft, Novell, Red Hat, Sun Microsystems und andere OPSEC-zertifizierte LDAP-Partner
LDAP-Protokolle	LDAPS und LDAP
Vordefinierte, anpassbare Profile	Nutzt Negativ- und Positivlisten, um offensichtlich böswillige Absender zu blockieren und vertrauenswürdige Absender zuzulassen.
Unterstützung von LDAP-Gruppen	Statisch und dynamisch
Erweitertes Schema	Das erweiterte Check Point-Schema unterstützt das Kennwortmanagement und weitere anbieterspezifische Attribute.
Redundanz	Bietet die Möglichkeit zur Abfrage mehrerer LDAP-Server sowie die Möglichkeit zur Verteilung der Benutzer auf verschiedene LDAP-Server.
Grafische Oberfläche	Anzeige, Bearbeitung und Erstellung von Benutzern und Gruppen sowie weiteren Objekten über eine benutzerfreundliche Oberfläche

SmartProvisioning Software Blade

ÜBERSICHT

Das Check Point SmartProvisioning Software Blade ermöglicht die zentrale Administration und Bereitstellung von Check Point-Sicherheitssystemen über eine einzige Managementkonsole und vereinfacht damit die Verteilung vor Sicherheitsrichtlinien und Konfigurationseinstellungen auf eine große Anzahl von Geräten an verteilten Standorten Zusätzlich enthält das System einen zentralen Backup-Manager und ein Repository von Gerätekonfigurationen, su dass bestehende Konfigurationen leicht auf neue Geräte übertragen werden können.

VORTEILE

- Verringert den Administrationsaufwand
- Beschleunigt die Bereitstellung und den Austausch von Geräten
- Automatisiert das Gerätemanagement und senkt so die Fehlerhäufigkeit und steigert die Sicherheit
- Kontrolliert zentral die Bereitstellung, Wartung und Wiederherstellung von Appliances
- Bietet Skalierbarkeit für die Verwaltung tausender Geräte in verschiedenen, getrennten Netzwerken

LEISTUNGSMERKMALE

- Zentrale Konfiguration der Betriebssystem- und Netzwerkeinstellungen der Geräte sowie einfache Navigation zwischen Systemübersicht, Profilkonfiguration und Gerätekonfiguration
- Profilbasiertes Management großer Umgebungen durch die Erstellung gemeinsamer Sicherheitsrichtlinien und Geräteeinstellungsprofile. Diese Profile werden anschließend auf alle Gateways mit gleichen Eigenschaften übertragen, wodurch der Administrationsaufwand reduziert und die Genauigkeit der Konfiguration verbessert wird.
- Zentraler Bereitstellungs-Assistent für die schnelle Konfiguration bei der Bereitstellung einer großen Anzahl von Systemen
- Zeitgesteuerte Aktionen, um Vorgänge wie die Abarbeitung von Skripten, die Installation von Software-Paketen, das Erstellen von Backups, Neustarts, die Durchsetzung von Richtlinien, die Übertragung von Objekten usw. durchzuführen

INTERESSANT FÜR

- Kunden mit umfangreichen Check Point-Installationen
- Unternehmen mit über 1.000 Benutzern

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Zentrale Konsole zur Bereitstellung, Wartung und Sicherung von Geräten
- Schnellere Bereitstellung neuer Geräte
- Geringere Anzahl von Konfigurationsfehlern
- Standardeinstellungen für Geräte im gesamten Unternehmen

GESPRÄCHSEINSTIEG

- Verfügen Sie über Zweigstellen ohne einen speziellen Sicherheitsadministrator?
- Planen Sie, bereits vorhandene Gateways mit neuer Hardware aufzurüsten?

SmartProvisioning Software Blade

SPEZIFIKATIONEN

Funktion	Beschreibung
Einfache, intuitive Oberfläche	Ja (inklusive SmartProvisioning-Assistent)
Sicherung	Sofort und geplant
Konfiguration	Routing, DNS, Domäne, Schnittstellen, Datum und Uhrzeit (Edge) und DHCP (Edge)
Gemeinsame Konfiguration	Mit Hilfe von Profilen
Package-Management	Unterstützt
Benutzerdefinierte CLI	Unterstützt
Trennung von Konfiguration und Sicherheit	Berechtigung und spezielle Anwendung
Konfigurationsassistent	Ja
Ausführung von Skripten und vordefinierten Operationen	Ja
Konfiguration auslesen	Ja (nur SecurePlatform)
Übersicht und Statusanzeige	Ja
Management von Gerätesoftware	Ja
Administratorzugriff für Steuerung	Ja
Geplante Aktionen	Nein
Vorübergehende Deaktivierung des zentralen Managements	Ja

SmartReporter Software Blade

ÜBERSICHT

Das Check Point SmartReporter Software Blade verwandelt die umfangrei-chen Datenmengen, die von Sicherheitssystemen und Netzwerkgeräten gesammelt werden, in verständliche, nachvollziehbare Informationen. Mit Hilfe dieser Informationen können Unternehmen die Effektivität ihrer Sicherheitsrichtlinien und -maßnahmen überprüfen, die Netzwerkkapazität planen und ihre Sicherheitsinvestitionen optimieren.

VORTEILE

- Veranschaulicht den Wert der Sicherheitsinvestitionen
- Reduziert den mit dem Management verbundenen Zeit- und Kostenaufwand
- Verbessert die Wahrnehmbarkeit von Sicherheitsbedrohungen
- Bietet Berichtsfunktionen für Audits und die Einhaltung gesetzlicher Vorschriften
- Vordefinierte Berichtsvorlagen

LEISTUNGSMERKMALE

- Die zentrale Berichterstattung umfasst eine Reihe vordefinierter Berichte, die in einfach zu verwendenden Kategorien organisiert sind. Zusätzlich können auch schnell benutzerdefinierte Berichte erstellt werden
- Mit Hilfe der automatischen Verteilung von Berichten und Datenbank-pflege können Berichte per E-Mail an bestimmte Benutzer gesendet oder auf FTP-Server oder Websites hochgeladen werden
- Dank Skalierbarkeit und flexiblen Bereitstellungsoptionen kann die Berichtsfunktion für das globale Netzwerk, für bestimmte Netzwerkseg-mente oder zur Berichterstattung für Kunden konfiguriert werden. Außer-dem ermöglicht sie den Parallelbetrieb mehrerer Reporting-Blades
- Einfache Trenderstellung und Analyse dank effizienter kontinuierlicher Erfassung von Sicherheits- und Netzwerkinformationen
- Die Berichte zur Einhaltung gesetzlicher Vorschriften werden an die relevanten Anforderungen der PCI-, SOX-, HIPAA-, COBIT- und ISO 27002-Vorschriften und -Standards angepasst

INTERESSANT FÜR

- Check Point-Kunden mit drei oder mehr Gateways
- Finanzdienstleister und Gesundheits-unternehmen, Bildungseinrichtungen, Produktionseinrichtungen und Managed Security Service Provider

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Bietet grafische, benutzerfreundliche Berichte, die als leistungsfähige Entschei-dungshilfe dienen
- Stellt Daten vom Desktop-Ereignis bis hin zum Perimeter-Ereignis in konsistenter Weise dar
- Bietet eine Vielzahl vordefinierter Berichte, die leicht angepasst werden können
- Skalierbar bis hin zu Provider-1-Umge-bungen (Multi-Domain-Management-Umgebungen)

GESPRÄCHSEINSTIEG

- Wie viel Zeit wenden Sie für die Verwaltung von Protokollen auf?
- Verfügen Sie über automatisierte Verfahren, um Berichte aus den Daten mehrerer Sicherheitssysteme zu generieren?
- Suchen Sie nach einer skalierbaren Berichtslösung?

SmartReporter Software Blade

SPEZIFIKATIONEN

Funktion	Beschreibung
Sichere Erfassung von Protokollen	Agent-basiert mit Hilfe der sicheren Check Point OPSEC LEA API
Konsolidierung von Protokollen	Kombiniert Instanzen mit gleichen Hauptinformationen, um die Daten zu komprimieren.
Anpassbare Konsolidierungsrichtlinie	Management über SmartDashboard
Vordefinierte Berichte	Große Anzahl vordefinierter Berichte zur Sicherheits-, Firewall- und Netzwerkaktivitäten, zum Status von Endpunkten sowie zur Aktivität des Antivirus-Schutzes
Expressberichte	Berichte, die auf SNMP-ähnlichen Zählern und Protokolldateien basieren
Standardberichte	Berichte, die auf konsolidierten Protokolldateien basieren
Automatische Wartung	
Kurzfristige Speicherung	Standardmäßig 60 Tage
Langfristige Speicherung	Ja, je nach Hardware
Datenbank	SQL
Ereignisse pro Sekunde	Bis zu 6.000
Management Blade und Multi-Domain Management Blade-Unterstützung	Unterstützt globales und kundenspezifisches Reporting
Automatische Verteilung von Berichten	Unterstützt globales und kundenspezifisches Reporting
Anpassung von Berichten	Berichtsinhalt, im Bericht enthaltener Zeitabschnitt, Eingangsquellen, Inhaltswerte von Filtern, Planung von Berichten, Ausgabeformat und Anzeige von Beispielberichten
Anpassung der Protokollkonsolidierung	Vom Anfang oder vom Ende her oder für bestimmte Protokolldateien
Rollenbasierte Administration	Synchronisierung mit dem Management Blade
Standardisiertes Reporting	Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) und Federal Information Security Management Act (FISMA), Basel II sowie das Cardholder Information Security Program von Visa (CISP)
Unterstützte Steuerungs-Frameworks	Control Objectives for Information Technology (COBIT) und ISO 27002

Smart Event Software Blade

ÜBERSICHT

Das Check Point Smart Event Software Blade ermöglicht die zentrale Korrelation und Verwaltung von Sicherheitsereignissen in Echtzeit. Dabei werden sowohl Sicherheitsereignisse von Check Point Sicherheits-Gateways als auch Sicherheitsereignisse auf Systemen von Drittanbietern verarbeitet. Die automatische Aggregation und Korrelation von Daten trägt nicht nur zu einer deutlichen Reduzierung der für die Analyse aufgewendeten Zeit bei, sondern isoliert darüber hinaus die wirklichen Sicherheitsbedrohungen und konzentriert sich auf diese.

VORTEILE

- Übersetzt Sicherheitsereignisse in Handlungsempfehlungen
- Identifiziert schnell vorher nicht erkennbarer Aktivitäten
- Reduziert das Geschäftsrisiko durch Reaktion in Echtzeit
- Konzentriert die Ressourcen auf die kritischsten Bedrohungen
- Niedrige TCO dank einfacher Installation und Bereitstellung
- Steigert den Nutzwert der aktuellen Sicherheitsinvestitionen

LEISTUNGSMERKMALE

- Die skalierbare, verteilte Architektur ist in der Lage, Millionen von Protokollen pro Tag und Korrelationseinheit zu verarbeiten. Zusätzlich verfügt sie über die Fähigkeit, die Arbeitsbelastung auf mehrere Korrelationseinheiten zu verteilen, so dass sie auch für große Unternehmensnetzwerke geeignet ist.
- Die zentrale Ereigniskorrelation nutzt sichere Verbindungen, um die Protokolldaten von Check Point- und Drittanbieter-Geräten in Rohform zu erfassen. Anschließend werden diese Daten an zentraler Stelle aggregiert, normalisiert, korreliert und analysiert.
- Die Bereitstellung ist dank der engen Integration mit den SmartCenter- und Provider-1-Protokollservern von Check Point sehr einfach. Der Event Correlation-Blade lernt automatisch die Netzwerktopologie und erkennt korrelierte Ereignisse, die für topologische Parameter von Bedeutung sind.
- Einfache Wartung dank eines Lernmodus, der ein grundlegendes Regelwerk für das normale Aktivitätsmuster eines Standorts erstellt und anschließend Richtlinienänderungen zur Feinanpassung des Systems vorschlägt

INTERESSANT FÜR

- Check Point-Kunden, die eine Sicherheitsereignis-Managementlösung (SIEM) in Betracht ziehen oder evaluieren
- Große und mittelgroße Unternehmen
- Finanzdienstleister, Bildungsbereich, Gesundheitswesen, Produktion und Managed Security Service Provider

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Einfache Bereitstellung und Wartung dank vordefinierter Ereignisse und Lernmodus
- Integration in SmartCenter und Provider-1 ermöglicht das automatische Erlernen der Netzwerktopologie und die Erkennung korrelierter Ereignisse, die für topologische Parameter von Bedeutung sind
- Möglichkeit zur Einbindung zusätzlicher Korrelationseinheiten für Umgebungen, die erhöhte Leistung benötigen

GESPRÄCHSEINSTIEG

- Auf welche Weise analysieren Sie gegenwärtig Ihre Protokolldaten?
- Wie erfüllen Sie interne und externe Auditing-Anforderungen?
- Wie priorisieren Sie gegenwärtig Sicherheitsereignisse?

Smart Event Software Blade

SPEZIFIKATIONEN

Datenquellen	
Unterstützte Produkte	Blue Coat, Check Point, Cisco, Fortinet, Industry Standard, ISS Juniper, McAfee, Microsoft, NetContinuum, Nortel, Open Source, Sun Symantec, TippingPoint, Top Layer, TrendMicro
Grafische Protokoll-Analyse	Grafische Protokoll-Analyse zum Auslesen von Drittanbieter-Log-Files
Verschiedene Protokollerfassungsmethoden	Agentenbasierte und agentenlose Protokollerfassung
Transparenz	
Ansichten mit Zeitachsen	Anzeige von echtzeitbasierten Informationen, Trends und Anomalien auf einen Blick, wobei Sicherheitsereignisse grafisch aufbereitet werden, um Anzahl, Zeitpunkt und Schwere der Ereignisse zu verdeutlichen
Diagrammansichten	Anzeige von Security-Events in Balken- oder Kreisdiagrammen
Karten	Geografische Lokalisierung von Quell- oder Ziel-IP auf Landkarten
Schnellansichten für Ereignisse	Unmittelbare Gruppierung von Ereignissen nach wichtigen Ereignistypen, Ereignisquellen, Zielen, Benutzern und Ländern
Analyse von Sicherheitsereignissen	
Auf Basis von Security-Events und Best Practices basierte Correlation	Konvertiert die Protokolle von Drittanbietern in Check Point-Format.
Anpassbare Sicherheitsereignisse	Individuelle Erstellung von Korrelationsregeln zur Überwachung aller Sicherheitsereignisse
Forensik	Genaue Suche nach Ereignisdaten durch Doppelklicken auf Zeitachsen, Diagramme oder Karten; schnelle Datenanalyse bis auf Paketebene
Ereignisgruppierung und -suche	Einfache Suchfunktionen und Datengruppierung für die Ereignisanalyse
Identitätserfassung	Verknüpfung von IP-Adresse und Benutzername anhand von Active Directory
Client-Info-Anwendung	Umfassende Gerätedaten (zu Prozessen, Hot Fixes und Schwachstellen) für beliebige Geräte durch Rechtsklick auf die Geräte-IP
Intelligenter Lernmodus	Baseline-Aktivitäten zur Erkennung normaler Trends
Schwachstellenanalyse bei Sicherheitsereignissen	Integrierte Schwachstellenanalyse für ausgewählte Sicherheitsereignisse
Praxisorientierte Sicherheit	
Event Ticketing	Zuweisung von Ereignissen an Administratoren mit dem Ticketing-Workflow
Globale und ereignisspezifische Ausnahmen	Anpassung von Warnungen mit Ausnahmen für Produkte, Quellen, Ziele und Services
Praxisorientierte Sicherheit	Automatische oder manuelle Bearbeitung von Sicherheitsereignissen und Änderung von Sicherheitsrichtlinien anhand der Ereignisanalyse
Verschiedenes	
Skalierbare, verteilte Architektur	Protokollserver, Ereigniskorrelationsserver und Ereignisserver lassen sich in separaten Systemen bereitstellen
Sofort einsatzbereite Appliance-Lösung	Appliance-basierte Lösung für eine einfache Bereitstellung
Pakete	
Vollständiges SmartEvent-Paket	Zentrale Korrelation und Verwaltung von Sicherheitsereignissen in Echtzeit für alle Check Point-Produkte und für Geräte von Drittanbietern
SmartEvent Intro	Zentrale Korrelation und Verwaltung von Sicherheitsereignissen in Echtzeit für ein Check Point Security Software Blade

Multi-Domain Security Management

ÜBERSICHT

Sorgen Sie für mehr Sicherheit und Kontrolle, indem Sie Ihr Sicherheits-management auf mehrere virtuelle Domänen aufteilen. Davon können Unternehmen jeder Größe profitieren. Erstellen Sie bequem virtuelle Domänen, die auf Standorten, Abteilungen oder Sicherheitsfunktionen basieren, um den Schutz zu verbessern und das Management zu vereinfachen.

VORTEILE

- Vereinfachte Verwaltung und Bereitstellung von Sicherheitsfunktionen in komplexen Umgebungen
- Mehr Sicherheit dank zentraler Konfiguration für VPN, Firewall, IPS sowie aller anderen Blades
- Verbesserte Effizienz durch Konsolidierung von Infrastruktur und Ressourcen für das Sicherheitsmanagement
- Einheitliche Sicherheitsrichtlinie, die mit dem Global Policy Software Blade in verschiedenen Domänen implementiert werden kann
- Einfacher Umstieg von Provider-1 oder bestehendem Management auf Multi-Domain-Management

LEISTUNGSMERKMALE

- Multi-Domain-Management für unterschiedliche Regelwerke
- Zentrales, unabhängiges Sicherheitsmanagement und Überwachung für alle virtuellen Domänen
- Granulare, rollenbasierte Administration für mehr Präzision
- Sichere Kommunikation zwischen allen Multi-Domain-Komponenten
- Flexible Multi-Domain Software Blades setzen auf vorhandenes Sicherheitsmanagement auf

INTERESSANT FÜR

- Große Unternehmen, die sich gegenwärtig im Prozess der Übernahme oder der Fusion mit einer anderen Firma befinden, über mehrere Standorte und eine komplexe Sicherheitsrichtlinie verfügen oder eine Vielzahl kleinerer Zweigstellen besitzen
- ISP, Kommunikationsunternehmen, Finanzdienstleister und Produktionseinrichtungen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Höchste Flexibilität durch Richtlinienmanagement auf verschiedensten Ebenen
- Granulare, rollenbasierte Administration für bessere Skalierbarkeit des Managements
- Ermöglicht virtuelles Management und virtuelle Datenbankumgebung für jeden Kunden
- Modulare, skalierbare Architektur, mit der Administratoren problemlos Hunderte neuer Kunden hinzufügen können
- Integriertes Management physischer und virtueller Sicherheits-Gateways

GESPRÄCHSEINSTIEG

- Wie verwalten Sie Ihre globalen Sicherheitsrichtlinien über verschiede SmartCenter hinweg?
- Verfügen Sie über mehrere Sicherheitsmanagement-Umgebungen?
- Möchten Sie für alle Sicherheitsgateways eine einheitliche Sicherheitsrichtlinie durchsetzen?
- Wollen Sie Ihr Sicherheitsmanagement anhand von geografischen Standorten, Geschäftsaufgaben und/oder individuellen Sicherheitsanforderungen aufteilen?

SPEZIFIKATIONEN: ANFORDERUNGEN DES MULTI-DOMAIN SECURITY MANAGEMENT SERVER

Komponente	Linux	Solaris	SecurePlatform
CPU	Intel Pentium-Prozessor E2140 oder äquivalenter Prozessor mit 2 GHz	UltraSPARC III 900MHz	Intel Pentium-Prozessor E2140 oder äquivalenter Prozessor mit 2 GHz
Arbeitsspeicher	4 GB	4 GB	4 GB
Festplattenspeicher	2 GB	2 GB	10 GB (Installation umfasst OS)
CD-ROM-Laufwerk	Ja	Ja	Ja (bootfähig)

Multi-Domain Security Management

HARDWARE-ANFORDERUNGEN DER MULTI-DOMAIN SECURITY CONSOLE

Komponente	Windows
CPU	Intel Pentium-Prozessor E2140 oder äquivalenter Prozessor mit 2 GHz
Arbeitsspeicher	512 MB
Festplattenspeicher	500 MB
Video-Adapter	Mindestauflösung: 1024 × 768

SMART-1: HARDWARE-SPEZIFIKATION

Smart-1-Appliances	50	150
Management HA	Enthalten	Enthalten
Protokolle/s	30.000	30.000
Festplattenspeicher	4 x 1 TB	4 x 1 TB; bis zu 12 TB
Speichertyp	RAID 10	RAID 10
Fibre Channel-SAN-Karte	Optional	Optional
Out-of-band-Management	Integriert	Integriert
Gehäuse	2 U	3 U
Integrierte Schnittstellen	4 Kupfer-GbE	4 Kupfer-GbE
Abmessungen (Zoll)	22,8 × 17,4 × 3,5 Zoll	24,9 × 17,4 × 5,2 Zoll
Abmessungen (metrisch)	580 × 442 × 88 mm	632 × 442 × 131 mm
Gewicht	23,5 kg (51,8 lbs)	29,5 kg (65 lbs)
LCD-Anzeige	■	■
Netzteile	2	3
Netzeingang	90–264 VAC @ 47–63 Hz	90–264 VAC @ 47–63 Hz
DC-Option	■	-
Spezifikation der Stromversorgung (max.)	2 x 600 W	3 x 930 W
Betriebsumgebung	Temperatur: Umgebung 0–40 °C; relative Luftfeuchtigkeit: 5 bis 95 % (nicht kondensierend)	
Compliance	CE, FCC Klasse A, RoHS	
Secure OS	Vorgehärtetes, optimiertes Betriebssystem	
Webbasierte Administration	Schnelle, einfache und sichere Verwaltung von jedem Punkt im Netzwerk aus	
Backup und Wiederherstellung	Zur Disaster Recovery-Planung	
Zentrale Administratorrechte	RADIUS-Authentifizierung und RADIUS-Gruppen	

SMART-1 MANAGEMENT SOFTWARE BLADES

Komponente	Linux	Solaris
Verwaltete Gateways	■	■
Verwaltete Domänen	■	■
Network Policy Management	■	■
Endpoint Policy Management	■	■
Logging und Status	■	■
SmartProvisioning	■	■
Monitoring	■	■
User Directory	■	■
SmartEvent Intro	■ *	■ *
Management Portal	Optional	Optional
SmartWorkflow	Optional	Optional
SmartEvent	Optional*	Optional*
SmartReporter	Optional*	Optional*
Multi-Domain Security Management (Provider-1)	Optional*	Optional*

* Nicht unterstützt bei Smart-1-Appliances, auf denen Multi-Domain Security Management läuft

Check Point Endpoint Security

Check Point Endpoint Security bietet Endpunktsicherheit auf höchstem Niveau, ohne den Bedienkomfort für Endanwender zu beeinträchtigen. Erstklassige Datenschutzfunktionen beugen dem Verlust von Unternehmensdaten vor, während gemeinsam genutzte Endpunkt- und Netzwerksicherheitsfunktionen die Komplexität reduzieren und die Kosten senken.

Check Point Endpoint Security

Check Point Full Disk Encryption™ und Media Encryption

Check Point GO

Endpoint Security

Vollständige Sicherheit durch einfach zu bedienende Endpoint Security und Datenschutzfunktionen

ÜBERSICHT

Check Point Endpoint Security™ ist der erste und einzige Client, der alle wichtigen Komponenten für umfassende Endgerätesicherheit kombiniert, ohne dabei die Funktionalität für den Endanwender zu beeinträchtigen. Erstklassige Datenschutzfunktionen beugen dem Verlust von Unternehmensdaten vor, während gemeinsam genutzte Endpoint- und Netzwerksicherheitsfunktionen die Komplexität reduzieren und die Kosten senken. Zu den Alleinstellungsmerkmalen zählen Check Point WebCheck™, das Endgeräte vor webbasierten Angriffen schützt, und Check Point OneCheck™, welches eine Single-Sign-On-Funktion bietet.

VORTEILE

- Umfassende Kontrolle aller Bedrohungsformen am Endgerät in einem einzigen Client, der mehr als 10 verschiedene Funktionen vereint, darunter Anti-Malware-Schutz, Firewall, NAC, VPN, Datenverschlüsselung und Portkontrolle
- Innovative Technologie mit Check Point WebCheck™ für sichere Internetnutzung, welches Drive-By-Downloads und Phishing-Attacken blockiert
- Erstklassige Datensicherheit mit den besten verfügbaren Verschlüsselungs- und Zertifizierungsverfahren
- Transparente, leistungsstarke Bedienmöglichkeiten für Endbenutzer durch eine einheitliche Oberfläche, Single-Sign-On, Infobereichssymbol, Anti-Malware-Prüfung und Client-Update
- Gemeinsam genutzte Netzwerk- und Endpunktsicherheit für stärkeren und einfacheren Schutz

LEISTUNGSMERKMALE

- Single Endpoint Security Agent – Kompletter Schutz für Endgeräte in einem einzigen Client, der Endpunktsicherheit, Datenschutz und Remote Access vereint. Nach der Installation wird nur ein Minimum an Speicherplatz benötigt.
- Firewall und Anti-Malware-Scan – Blockiert unerwünschten Datenverkehr und erkennt Malware. Die Schutzfunktionen bieten die höchste Scangeschwindigkeit der Branche und den geringsten Speicherverbrauch (vor und während des Scans sowie danach).
- NAC und VPN – Setzt die Endpunktrichtlinie sowohl für den VPN-basierten als auch für den internen Netzwerkzugriff durch. Die VPN Auto-Connect-Funktion hält die Verbindung beim Wechsel zwischen verschiedenen Netzwerken aufrecht.
- Zentrales Management – Ermöglicht die zentrale Konfiguration, Verwaltung und Analyse der Endpoint-Security-Funktionen und -aktivitäten sowie die zentrale Berichterstattung. Die zentrale Verwaltung von Regeln und Protokollierung ermöglicht schnelles Auditing und schnelle Berichterstattung zur Einhaltung von Vorschriften.
- Datensicherheit – Full Disk Encryption und Media Encryption bieten Sicherheit auf höchstem Niveau für Daten, die auf Laptops und Wechselmedien gespeichert sind. Die Verschlüsselung ist dabei für den Endbenutzer transparent.

INTERESSANT FÜR

- Unternehmen mit einer wachsenden Anzahl mobiler Mitarbeiter
- Unternehmen, die sich Sorgen um die Einhaltung der Datenschutzbestimmungen machen
- Unternehmen, die Datensicherheits- oder Antivirusprodukte durch das Produkt eines Mitbewerbers ersetzen möchten
- Unternehmen, die eine Ergänzung um zusätzliche Endpunktsicherheitskomponenten innerhalb der nächsten 6 Monate planen
- Unternehmen, die sich Sorgen darüber machen, dass mobile Mitarbeiter oder Gastmitarbeiter Probleme mit dem Netzwerkzugriff bekommen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Erster und einziger Single Endpoint Security Agent für umfassende Endpunktsicherheit
- Einfache und schnelle Anwendung dank geringstem Speicherplatzbedarf auf der Festplatte nach der Installation und schnellster Antivirusscan mit geringstem Arbeitsspeicherbedarf
- Einzigartige Browser-Sicherheit dank Check Point WebCheck – extrem schnelle Webseiten-Downloads bei aktivierter Browser-Sicherheit
- Hoch skalierbare Lösung – bewährt in Datensicherheits-Bereitstellungsszenarien mit mehr als 200.000 Arbeitsplätzen bei einer Wachstumsrate von 50.000 Arbeitsplätzen pro Monat
- Sicherheitszertifizierungen auf höchstem Niveau, darunter FIPS-140-2, CC EAL4, BITS und CESG CCTM

GESPRÄCHSEINSTIEG

- Wenn Sie an die neuesten Angriffsszenarien denken: Wenn Ihre Endpunktsicherheitslösungen Lücken aufweisen, wo würden Sie diese vermuten?
- Bis zu welchem Grad erfüllen Sie Ihre gesetzlichen SOX-, PCI- oder HIPAA-Vorschriften?
- Wie hat sich die kürzliche Krise auf Ihr allgemeines IT- und Sicherheitsbudget ausgewirkt?
- Welche Initiativen verfolgen Sie, um den Instandhaltungsaufwand (OPEX) und den Kapitaleinsatz (CAPEX) zu reduzieren?
- Bis zu welchem Grad beschweren sich Ihre Benutzer über die vorhandene Endpoint-Sicherheitsumgebung?

Endpoint Security

Vollständige Sicherheit durch einfach zu bedienende Endpoint Security und Datenschutzfunktionen

SPEZIFIKATIONEN

Unterstützte Clientplattformen	
Betriebssysteme	• Windows 7 (32 und 64 Bit) • Windows Vista (32 und 64 Bit) • Windows XP Pro (SP2, SP3)
Unterstützte Managementplattformen	
Betriebssysteme	• Windows Server 2003 • Check Point SecurePlatform™
Browser	• Internet Explorer 6, 7, 8 • Mozilla Firefox 1,5 oder höher
Check Point WebCheck	
Unterstützte Browser	• Microsoft Internet Explorer 6, 7, und 8 • Mozilla Firefox 2 und 3
Sprachunterstützung für Clients	
Sprachen	Englisch, Japanisch, Französisch, Italienisch, Deutsch, vereinfachtes Chinesisch, Spanisch und Russisch
Zertifizierungen	
Zertifizierungen	FIPS 140-2, Common Criteria EAL4, BITS und CESG CCTM

Full Disk Encryption

Festplattenverschlüsselung für mobile Rechner & Desktops

ÜBERSICHT

Das Check Point Full Disk Encryption Software Blade bietet automatische Sicherheit für alle Daten, die sich auf Festplatten von Endgeräten befinden, einschließlich Benutzerdaten, Betriebssystemdateien und gelöschter Dateien. Zur sicheren Anmeldung unterstützt FDE Multi-Faktor-Authentifizierung.

VORTEILE

- Schützt vor unberechtigten Zugriffen bei Diebstahl oder Verlust von Laptops
- Unterstützung der gängigen Sicherheitszertifikate: FIPS, Common Criteria, BITS
- Umfassende Plattformunterstützung inklusive Windows, Mac OS X und Linux
- Bewährt in Datensicherheitsumgebungen mit mehr als 200.000 Plätzen
- Schnelle Bereitstellung – bis zu 50.000 Plätze pro Monat
- Im „Magic Quadrant“ von Gartner als führende Lösung für mobile Datensicherheit geführt
- Kombination von vollständiger Festplattenverschlüsselung auf Endgeräten mit anderen Endpoint Security Software Blades möglich
- Zentrale Verwaltungslösung mit nur einer Konsole für alle Endgeräte

LEISTUNGSMERKMALE

Full Disk Encryption

Verschlüsselt automatisch alle Daten auf der Festplatte (zum Beispiel Benutzerdaten, Betriebssystem, temporäre Dateien und gelöschte Dateien) und sorgt so für maximale Datensicherheit.

Logische Partitionen werden beim Booten geschützt und Sektor für Sektor verschlüsselt. Versuche, einzelne Dateien zu kopieren oder schädliche Programme zu installieren, werden blockiert, selbst wenn die Festplatte entfernt und als Slave auf einem anderen Computer genutzt wird.

Pre-Boot-Authentifizierung

Stellt sicher, dass ausschließlich autorisierte Benutzer auf das Endgerät zugreifen. Bevor das Betriebssystem startet, müssen alle gültigen Anmeldedaten eingegeben werden. Die Lösung unterstützt Multi-Faktor-Authentifizierung wie zertifikatbasierte Smartcards sowie dynamische Token. Für globale Umgebungen wird die Pre-Boot-Authentifizierung in verschiedenen Sprachen unterstützt.

Zentrale Konsole mit intuitiver Benutzeroberfläche

Das Full Disk Encryption Endpoint Software Blade bietet eine intuitive Benutzeroberfläche für die zentrale Verwaltung und bequeme Anzeige von Sicherheitsstatus und Protokolldateien. Auch grundlegende Konfigurationsänderungen sind hier möglich.

Für globale Umgebungen werden verschiedenen Client-Sprachen unterstützt.

Sichere Remote-Hilfe

Benutzer, die ihr Kennwort vergessen oder den Token verloren haben, können das Kennwort über die Remote Passwortänderung ändern oder die Funktion Einmalanmeldung nutzen. Zudem sind webbasierte Remote-Hilfe-Optionen verfügbar.

SPEZIFIKATIONEN

Unterstützte Client-Plattformen		
Betriebssysteme	• Windows 7 (32/64 Bit) • Windows Vista (32/64 Bit) • Windows XP Pro (32 Bit, SP2, SP3) • Windows 2000 • Mac OS X (10.4.5 bis 10.4.11, 10.5.0 bis 10.7) • Linux (2.6.4+ Kernel, Red Hat, SuSE 9.x, RHEL 4, NLD)	
Unterstützte Client-Sprachen		
Sprachen	• Englisch • Japanisch • Französisch • Italienisch	• Deutsch • Chinesisch (vereinfacht) • Spanisch • Russisch
Unterstützte Sprachen bei der Pre-Boot-Authentifizierung		
Alle Client-Sprachen plus:	• Chinesisch (Taiwan) • Tschechisch • Französisch (Kanada) • Ungarisch • Koreanisch	• Polnisch • Portugiesisch • Portugiesisch (Brasilien) • Thailändisch
Zertifizierungen		
Full Disk Encryption	• Common Criteria EAL4 • FIPS 140-2	
Managementplattform		
Siehe Endpoint Policy Management Software Blade		

Media Encryption

Verschlüsselung externer Medien und Management von Ports

ÜBERSICHT

Das Check Point Media Encryption Software Blade bietet eine zentral durchsetzbare Verschlüsselung von austauschbaren Speichermedien wie USB-Flash-Laufwerken, Externen-Festplatten, CDs und DVDs und sorgt somit für maximale Datensicherheit. Mithilfe des Port-Management lassen sich alle Ports von Endgeräten verwalten. Zudem werden Port-Aktivitäten zentral erfasst, um Audit- und Compliance-Anforderungen zu erfüllen.

VORTEILE

- Verschlüsselung von Dateien und Ordnern; individuelle Verfolgung und Verwaltung austauschbarer Geräte
- Automatische und transparente Verschlüsselung von DVDs und CDs, die mit PCs erstellt werden
- Flexible Erweiterung der Endpoint-Sicherheit mit den Endpoint Security Software Blades
- Hohe Geschwindigkeit bei erstmaligem und wiederkehrenden Scans
- Minimale Speichernutzung
- Zentrale Richtliniendurchsetzung für Wechselmedien sowie Regeln für die Portnutzung
- Zentrale Protokollierung von Mediennutzung und Datenbewegungen

LEISTUNGSMERKMALE

Einrichtung von Verschlüsselung mit einer zentralen Sicherheitsverwaltung

Mit dem zentralen Endpoint Security Management können Administratoren Verschlüsselungsrichtlinien für Wechselmedien einrichten und durchsetzen. Dabei können Sie Algorithmen wie AES 256-Bit verwenden, um für optimale Datensicherheit zu sorgen. Mit Check Point können Benutzer auch über nicht verwaltete Computer und ohne Endpoint-Client sicher auf verschlüsselte Medien zugreifen.

Einstellungen für den Gerätezugriff

Mit den Einstellungen für den Gerätezugriff lässt sich die Nutzung von Wechselmedien und Ports steuern. Wechselmedien können anhand von Typ, Marke, Größe oder Seriennummer genau definiert werden. Der Zugriff auf Ports von Endgeräten (USB, FireWire, Bluetooth, WiFi, Drucker usw.) lässt sich zentral verwalten.

Protokolle und Warnungen

Administratoren können Protokolle zu Geräteaktivitäten und Dateibewegungen in einer zentralen Datenbank speichern, um diese für zuverlässige Compliance sowie einheitliche Auditing- und Berichterstellungsfunktionen zu nutzen. Zudem können E-Mail-Warnungen konfiguriert werden, um Administratoren über spezifische Aktivitäten zu informieren.

SPEZIFIKATIONEN

Unterstützte Client-Plattformen		
Betriebssysteme	• Microsoft Windows 7 Enterprise, Professional, Ultimate Editions (32/64 Bit und SP1) • Windows XP Pro (32 Bit, SP3 und höher) • Windows Vista 32/64 Bit	
Integration von CD-/DVD-Brennsoftware		
Anwendungen	• Windows CD/DVD-Assistent • Nero 9 Multimedia Software	
Unterstützte Client-Sprachen		
Sprachen	• Englisch • Japanisch • Französisch • Italienisch	• Deutsch • Chinesisch (vereinfacht) • Spanisch • Russisch
Zertifizierungen		
Zertifikate für die Medienverschlüsselung	• Common Criteria EAL4 • FIPS 140-2 • CCTM CESG	
Kontrollierte Ports		
Port-Typen	USB, WiFi, FireWire, IDE, Bluetooth, PS/2, PCMCIA, SATA, IrDA und SCSI	
Kontrollierte Geräte		
Gerätetypen	USB-Flash-Laufwerke, Diskettenlaufwerke, externe Festplatten, Bandlaufwerke, Windows Mobile-Smartphones, PDAs, Bildgeräte, Scanner, iPhones, Blackberrys, Modems, andere Netzwerkgeräte, iPods, andere digitale Musikgeräte, Drucker, CD/DVD-Laufwerke, Tastatur, Maus, Digitalkameras, Drahtlosnetzwerkkarten, biometrische Geräte und Smartcard-Leser	
Managementplattform		
Siehe Endpoint Policy Management Software Blade		

AntiMalware & Program Control

Malware-Schutz und Applikationskontrolle am Endpoint

ÜBERSICHT

Das Check Point Anti-Malware & Program Control Software Blade sorgt mit einem einzigen Scanvorgang für eine effektive Erkennung und Entfernung von Malware auf Endgeräten. Viren, Spyware, Keylogger, Trojaner und Rootkits werden mithilfe von Signaturen, Verhaltensblockern und heuristischen Analysen identifiziert. Die Programmkontrolle sorgt dafür, dass auf Endgeräten ausschließlich zugelassene Programme ausgeführt werden können. Das Software Blade lässt sich mit dem zentralen Endpoint Security Management bequem verwalten.

VORTEILE

- Die branchenweit schnellste Scan-Lösung für Malware und Viren mit der kürzesten Boot-Zeit
- Minimaler Arbeits- und Festplattenspeicherbedarf
- Zentrales Management mit nur einer Konsole
- Identifizierung der Malware mithilfe von Signaturen, Verhaltensblockern und heuristischen Analysen
- Automatische Aktualisierung des Schutzes mit dem optionalen Program Advisor Service
- Wissensdatenbank mit über 1 Million kategorisierten Programmen

LEISTUNGSMERKMALE

Malware-Prüfung mit nur einem Scanvorgang

Das Anti-Malware & Program Control Software Blade sorgt mit einem einzigen Scanvorgang für eine effektive Erkennung und Entfernung von Malware auf Endgeräten. Viren, Spyware, Keylogger, Trojaner und Rootkits werden mithilfe von Signaturen, Verhaltensblockern und heuristischen Analysen identifiziert. Mit Anti-Virus-Funktionen stoppt das Anti-Malware & Program Control Software Blade Viren, bevor diese Endbenutzer erreichen und andere Geräte infizieren können.

Im Vergleich zu anderen führenden Anti-Malware-Lösungen zeichnet sich Check Point durch den schnellsten Initial- und wiederholten Scan sowie kürzeste Boot-Zeit und den geringsten Bedarf an Arbeits- und Festplattenspeicher aus.

Richtlinie für Malware- und Virenschutz

Die Richtlinie für Malware- und Virenschutz lässt sich mithilfe einer zentralen Konsole verwalten und bereitstellen, sodass Administratoren die Scan-Zeitplanung und alle Aspekte der Problembehandlung genau steuern können.

Programmkontrolle

Mit der Programmkontrolle wird sichergestellt, dass nur legitime und zugelassene Programme ausgeführt werden können. Die Echtheit von Programm wird verifiziert, um Spoofing, Änderungen oder das Hijacking von Anwendungen zu verhindern. Automatisch wird ein Inventar mit allen Anwendungen erstellt, die versuchen, auf das Netzwerk zuzugreifen. Nicht autorisierte Verbindungen sowie Datenübertragungen durch schädliche Programme werden blockiert.

Program Advisor Service: App Control

Der optionale Check Point Program Advisor Service liefert aus einer Datenbank, die über 1 Million vertrauenswürdige und verdächtige Programme umfasst, echtzeitbasierte Updates für das Anti-Malware & Program Control Software Blade.

AntiMalware & Program Control

Malware-Schutz und Applikationskontrolle am Endpoint

SOFTWARE BLADE: SPEZIFIKATION

Unterstützte Client-Plattformen		
Betriebssysteme	• Windows 7 (32/64 Bit) • Windows Vista (32/64 Bit) • Windows XP Pro (32 Bit, SP2, SP3)	
Unterstützte Client-Sprachen		
Sprachen	• Englisch • Japanisch • Französisch • Italienisch	• Deutsch • Chinesisch (vereinfacht) • Spanisch • Russisch
Managementplattform		
Siehe Endpoint Policy Management Software Blade		
Antivirus		
Heuristischer Viren-Scan	Prüft Dateien und erkennt Infektionen anhand der Verhaltensmuster von Viren	
Viren-Scan beim Zugriff	Prüft Dateien beim Öffnen, Ausführen oder Schließen und ermöglicht so eine sofortige Erkennung und Behandlung von Viren	
Umfassender Scan	Führt eine genaue Prüfung aller Dateien im ausgewählten Ziel aus	
Ziellaufwerke prüfen	Ermöglicht die Auswahl der zu prüfenden Verzeichnisse und Dateitypen	
Scan-Ausnahmen	Ermöglicht die Auswahl von Verzeichnissen und Dateierweiterungen, die nicht geprüft werden sollen	
Aktionen	Reparieren, Umbenennen, Quarantäne, Löschen	
Unterstützte Antivirus-Programme von Drittanbietern	McAfee VirusScan, Symantec Norton Antivirus, Trend Micro PC-cillin/OfficeScan, Sophos Anti-Virus, Computer Associates eTrustInnoculateIT, Computer Associates VET, Check Point Endpoint Security Antivirus, Kaspersky Antivirus, NOD32 Antivirus, AVG Antivirus, AVAST Antivirus, BitDefender Antivirus, F-Secure Antivirus, Panda Antivirus, Microsoft OneCare Antivirus	
Anti-Spyware		
Intelligenter Schnell-Scan	Untersucht die am häufigsten betroffenen Bereiche von Dateisystem und Registrierung auf Spuren von Spyware	
Scan des kompletten Systems	Prüft lokale Dateiordner und bestimmte Dateitypen	
Umfassender Scan	Prüft jedes Datenbyte auf dem Computer	
Ziellaufwerke prüfen	Ermöglicht die Auswahl der zu prüfenden Verzeichnisse und Dateitypen	
Scan-Ausnahmen	Ermöglicht die Auswahl von Verzeichnissen und Dateierweiterungen, die nicht geprüft werden sollen	
Aktionen	Reparieren, Umbenennen, Quarantäne, Löschen	

Firewall & Compliance Check

Desktop Firewall & Compliance-Überprüfung am Endpoint

ÜBERSICHT

Das Check Point Firewall & Compliance Check Software Blade schützt Endgeräte durch eine Kontrolle des eingehenden und ausgehenden Datenverkehrs sowie durch die Sicherstellung der Richtlinien-Compliance. Für ein einheitliches Management steht eine zentrale Konsole zur Verfügung. Definierbare Zonen und Sicherheitsstufen schützen Endgeräte vor nicht autorisierten Zugriffen. Die integrierte Stealth-Technologie macht Endgeräte für Angreifer unsichtbar. Das Software Blade lässt sich mit dem zentralen Endpoint Security Management bequem verwalten und ist kostenfreier Bestandteil des Endpoint Security Containers.

VORTEILE

- Die Desktop-Firewall schützt Endgeräte durch eine Kontrolle des eingehenden und ausgehenden Datenverkehrs
- Zentral festlegbare Datenverkehrskontrollen, Sicherheitsstufen und Stealth-Technologie
- Compliance Check stellt sicher, dass alle Endgeräte konform sind, bevor sie auf das Unternehmensnetzwerk zugreifen
- Einfache Aktivierung von Endpoint Firewall und Compliance Check auf beliebigen Endgeräten
- Zentrale Verwaltung und Bereitstellung
- Gemeinsame Objektdatenbank mit der Netzwerk-Firewall sorgt für eine einfache Inbetriebnahme

LEISTUNGSMERKMALE

Desktop-Firewall

Die Desktop-Firewall schützt die Integrität von Endgeräten durch eine Kontrolle des eingehenden und ausgehenden Datenverkehrs. Festlegbare Zonen und Sicherheitsstufen verhindern, dass Malware Endgeräte infiziert, sie wehren gezielte Angriffe ab und sperren unerwünschten Datenverkehr. Die Stealth-Technologie macht Endgeräte für mögliche Angreifer unsichtbar. Check Point nutzt dabei seine seit 17 Jahren führende Firewall-Technologie.

Compliance Check

Mit Compliance Check werden Endgeräte auf die Einhaltung von Sicherheitsrichtlinien des Unternehmens geprüft. Nicht konforme Systeme können zur Weiterbehandlung umgeleitet werden.

Administratoren können sicherstellen, dass Endgeräte auf Basis unterschiedlicher Aspekte konform sind – zum Beispiel:

- Endpoint Security Client-Software ist auf dem neuesten Stand
- Endpunkt verfügt über die aktuellen Service Packs des Betriebssystems
- Suche nach „verbotenen“ Anwendungen, die auf einem Endgerät ausgeführt werden oder installiert sind
- Suche nach autorisierten Anti-Malware-Anwendungen, Versionen und DAT-Updates

SPEZIFIKATIONEN

Compliance Check	
Anti-Malware-Programme und Versionen, die von Compliance Check geprüft werden	Check Point, Symantec, McAfee, Trend Micro, Kaspersky, Nod32, AVG, Avast, Sophos, Panda CA, Inoculate IT Engine, BitDefender, MS Forefront
Firewall-Optionen	
Konfigurationsoptionen	Eingehende Firewall, ausgehende Firewall, Stealth-Modus
Unterstützte Plattformen	
Betriebssysteme	Windows 7 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP Pro (32 Bit, SP2 und höher)
Unterstützte Client-Sprachen	
Sprachen	• Englisch • Japanisch • Französisch • Italienisch • Deutsch • Chinesisch (vereinfacht) • Spanisch • Russisch
Managementplattform	
Siehe Endpoint Policy Management Software Blade	

Remote Access VPN

Client VPN

ÜBERSICHT

Das Check Point Remote Access VPN Software Blade bietet Benutzern, die auf Reisen sind oder extern arbeiten, sicheren Zugang zu Unternehmensnetzwerken und -ressourcen. Datenschutz und Integrität von sensiblen Daten wird durch Multi-Faktor-Authentifizierung, Prüfung der System-Compliance von Endgeräten und die Verschlüsselung aller übertragenen Daten sichergestellt. **Nutzung zusammen mit dem IPSec VPN Software Blade (am Gateway).**

VORTEILE

- Vollständige IPSec VPN-Verbindung für starke Authentifizierung und Datenintegrität
- Prüfung der Compliance von Endgeräten als Schutz vor Malware und Eindringlingen
- Nahtloses Roaming zwischen Netzwerken und automatische Session-Konfiguration
- Wiederherstellung unterbrochener Verbindungen durch automatische Änderung des Verbindungsmodus
- Schutzfunktion für Remotezugriff mit Endgeräten auf beliebigen Check Point-Gateways
- Zentrale Verwaltung von Endgeräten

LEISTUNGSMERKMALE

VPN Auto-Connect

VPN Auto-Connect stellt unterbrochene Verbindungen durch eine automatische Änderung des Verbindungsmodus wieder her. So müssen sich Benutzer beim Roaming zwischen verschiedenen Netzwerktypen (LAN, WiFi, GPRS usw.) nicht jedes Mal erneut anmelden.

IPSec VPN

Das Check Point Remote Access Software Blade unterstützt vollständige IPsec VPN-Verbindungen und sorgt für starke Authentifizierung sowie hohe Datenintegrität und Vertraulichkeit. Unterstützung des NAT-T-Standards ermöglicht eine Übertragung zwischen statischen und dynamischen NAT-Geräten.

Multi-Faktor-Authentifizierung

Das Remote Access Software Blade bietet umfangreiche Authentifizierungsfunktionen inklusive:

- Benutzername und Kennwörter (einschließlich Kennwörter im Cache)
- SecurID
- Challenge/Response
- CAPI-Software und Hardware-Token

Compliance-Prüfung

Mit Compliance-Prüfungen werden Endgeräte automatisch auf Malware und verdächtige Aktivitäten sowie auf die Einhaltung von Sicherheitsrichtlinien des Unternehmens gescannt. Nicht konforme Endgeräte können zur Weiterbehandlung umgeleitet werden.

Secure Hotspot-Anmeldung

Dank der Secure Hotspot-Anmeldung können Administratoren selektiv Zugriff auf Anmeldeseiten für Hotspots gewähren. Die Anmeldeseiten werden für Benutzer automatisch geladen.

SPEZIFIKATIONEN

Unterstützte Client-Plattformen	
Betriebssysteme	Windows 7 (32/64 Bit) Windows Vista (32/64 Bit) Windows XP Pro (32 Bit, SP2 und höher)
Unterschiedliche IPSec VPN-Clients	Check Point Endpoint Security, Endpoint Security VPN R75, SecuRemote
Unterstützte Client-Sprachen	
Sprachen	• Englisch • Japanisch • Französisch • Italienisch • Deutsch • Chinesisch (vereinfacht) • Spanisch • Russisch
Unterstützte Gateways	
Check Point-Gateways	• Check Point 2200, 4000, 12000, 21400 und 61000 Appliances • Check Point Power-1 Appliances • Check Point IP Appliances • Check Point UTM-1 Appliances • Check Point IAS
Managementplattform	
Siehe Endpoint Policy Management Software Blade	

WebCheck

Browser Security

ÜBERSICHT

Das Check Point WebCheck Endpoint Software Blade schützt Unternehmen vor der wachsenden Zahl an webbasierten Bedrohungen. Bekannte und unbekannte Webbedrohungen wie Drive-by-Downloads, Phishing-Sites und Zero-Day-Angriffe werden dank Browservirtualisierung isoliert, während hochmoderne Heuristikmethoden Benutzer davon abhalten, gefährliche Webseiten zu besuchen. Das Software Blade lässt sich mit dem zentralen Endpoint Security Management bequem verwalten.

VORTEILE

- Zuverlässiger Schutz vor Drive-by-Downloads und anderen webbasierten Bedrohungen
- Hochmoderne Anti-Phishing-Funktionen und heuristische Website-Analysen warnen Benutzer vor gefährlichen Websites
- Der Dual-Browser-Modus schützt Unternehmensdaten auf Endgeräten vor Schadsoftware
- Umfassende Web- und Browser-Sicherheit für Endgeräte
- Flexible Lizenzierungsoptionen (jährlich oder unbefristet)
- Zentrale Verwaltung und Bereitstellung
- Koexistenz und Verwaltung mit anderen Software Security Blades

LEISTUNGSMERKMALE

Browser-Virtualisierung

Das WebCheck Endpoint Software Blade optimiert die Browser-Sicherheit durch eine Virtualisierung des Browsers und die Schaffung einer isolierten, geschützten Sandbox für den Webbrowser. So werden Unternehmensdaten vom Internet getrennt. Wenn ein Benutzer versehentlich eine infizierte Website besucht, die einen Drive-by-Download über den Browser verursacht, oder ein schädliches Plug-In heruntergeladen wird, entsteht kein permanenter Schaden. Der Angriff wird in der virtuellen Sandbox aufgefangen und gelöscht, sobald die Browser-Sitzung beendet wird.

Anti-Phishing

Durch den Abgleich von Signaturen und heuristische Analysen werden Benutzer vor Phishing-Seiten gewarnt. Die heuristische Erkennungs-Engine von Check Point ermittelt betrügerische Kopien von wichtigen Finanz-, Social Networking-, Webmail- und Einkaufswebsites.

Zusätzlich zur Browservirtualisierung hindert das WebCheck Endpoint Software Blade Benutzer daran, gefährliche Webseiten aufzurufen. Mithilfe einer dualen Engine, die eine Signaturdatenbank für Phishing-Websites sowie eine proprietäre heuristische Methode umfasst, werden Phishing-Webseiten zuverlässig erkannt. Die Signaturdatenbank wird kontinuierlich aktualisiert und bietet stets neuesten Schutz vor bekannten Phishing-Webseiten.

Check Point hat zudem eine heuristische Erkennungsmethode für Phishing entwickelt, mit der sich falsche und betrügerische Kopien von über 50 Finanz-, Social Networking-, Webmail- und Einkaufswebsites präventiv erkennen lassen. Mithilfe der heuristischen Anti-Phishing-Engine kann das WebCheck Endpoint Software Blade Bedrohungen identifizieren, bevor diese gemeldet und in die signaturbasierten Sperrlisten aufgenommen werden.

Prüfung des Websteiten-Status

Das WebCheck Endpoint Software Blade bewertet jede besuchte Webseite und warnt Benutzer, wenn eine Seite schwache oder verdächtige Merkmale aufweist. Zu diesem Zweck werden zahlreiche Attribute untersucht. Hierzu gehören das Alter der Domäne, eine mögliche Auflistung der IP-Adresse in öffentlichen Spam-Listen oder ein Hosting der Webseite in bestimmten Ländern.

SPEZIFIKATIONEN SOFTWARE BLADE

Unterstützte Browser	
Von WebCheck geschützte Browser	• Internet Explorer 6, 7, 8 • Mozilla Firefox 2, 3
Unterstützte Client-Plattformen	
Betriebssysteme	• Windows 7 (32/64 Bit) • Windows Vista (32/64 Bit) • Windows XP Pro (32 Bit, SP2 und höher)
Unterstützte Client-Sprachen	
Sprachen	• Englisch • Japanisch • Chinesisch (vereinfacht)
Managementplattform	
Siehe Endpoint Policy Management Software Blade	

WebCheck

Browser Security

BROWSER-SCHUTZ

Das WebCheck Endpoint Software Blade schützt Browser vor Angriffen in den folgenden Bereichen:

Ziel des Browser-Angriffs	Angriffsmethode
Externes Browser-Plug-In	Drive-by-Malware über ein Plug-In außerhalb des Browsers (Flash, Acrobat, Office usw.)
Internes Browser-Plug-In	Drive-by-Malware über ein Plug-In innerhalb des Browsers
Nicht behobene Schwachstellen	Drive-by-Malware über ein Leck im Browser
BHO (Browser Helper Object)	Drive-by-Malware über ein Plug-In außerhalb des Browsers

HEURISTISCHER PHISHING-SCHUTZ

Das WebCheck Endpoint Software Blade bietet für wichtige Webseiten präventiven heuristischen Phishing-Schutz.

Kategorie	Website (Beispiele)
Online-Banking	Bank of America Wachovia Wells Fargo
eCommerce	eBay PayPal Amazon
Social Networking & Webmail	MySpace Yahoo Mail MSN Hotmail

Check Point GO

Sicherer virtueller Arbeitsplatz

ÜBERSICHT

Mit Check Point GO können Sie Ihr Büro in Ihrer Tasche transportieren. Dies wird durch einen sicheren virtuellen Arbeitsplatz ermöglicht, der jeden beliebigen PC in Ihren eigenen Unternehmensdesktop verwandelt. Dank GO können Benutzer jederzeit und von jedem Ort aus auf Dateien und Anwendungen zugreifen – ohne sich mit sperrigen Laptops oder beruflichen Dateien belasten zu müssen.

VORTEILE

- Verwandeln Sie jeden beliebigen PC mit Hilfe eines einfachen, verschlüsselten USB-Sticks in Ihren eigenen Unternehmensdesktop
- Greifen Sie mit der integrierten VPN-Client-Funktion jederzeit und von jedem Ort aus auf Ihre beruflichen Dateien und Anwendungen zu
- Der sichere virtuelle Arbeitsplatz trennt die Daten vom Hostcomputer und kontrolliert gleichzeitig die Anwendungen und Dateiübertragungen
- Die integrierte Software- und Hardware-Verschlüsselung schützt Daten und Informationen sowohl bei der Arbeit als auch unterwegs
- Ideal für mobile Mitarbeiter, Subunternehmer, Partner und für Wiederherstellungspläne im Notfall

LEISTUNGSMERKMALE

- Schneller Start durch Plug-&-Play-Betrieb ohne Software-Installation und Reboot
- Standard-Windows®-Benutzerumgebung ermöglicht eine schnelle Eingewöhnung des Benutzers und schnelle Bereitstellung
- Virtualisierung, Kontrolle der Programme und Kontrolle des ausgehenden Datenverkehrs zur Vermeidung von Datenverlusten
- Zentrales Management ermöglicht die Verteilung von Richtlinien und Remote-Unterstützung bei Kennwortproblemen
- FIPS 140-2-zertifiziertes USB-Laufwerk für Hochsicherheitsanwendungen erhältlich

GESPRÄCHSEINSTIEG

- Wie viele Ihrer Mitarbeiter arbeiten von zu Hause oder mit ihren eigenen Computern?
- Wie viele Ihrer mobilen Mitarbeiter würden es bevorzugen, ohne einen sperrigen Laptop zu reisen?
- Welche Pläne haben Sie für Notfallsituationen (Epidemien, Naturkatastrophen)?
- Auf welche entscheidenden Daten müssen Ihre Mitarbeiter zugreifen können, wenn sie nicht ins Büro kommen können?
- Inwiefern haben sich Budgetengpässe auf die Erweiterung der Zahl Ihrer mobilen Mitarbeiter ausgewirkt?
- Inwiefern haben sich Budgetengpässe auf Ihre Pläne für die Wiederherstellung im Notfall ausgewirkt?

INTERESSANT FÜR

- Mittelgroße und kleine Unternehmen auf der ganzen Welt
- Gesundheitswesen, Finanzwesen, Behörden, große Unternehmen, Produktion
- Unternehmen, die PCI oder HIPAA benötigen oder geistiges Eigentum schützen müssen usw.
- Versicherungsbranche, Maklergewerbe
- Callcenter
- CSO, Security VP/Director innerhalb von Desktop-Administrationsgruppen
- CIO, VP/Director/Manager für IT, IS, MIS, Desktop- und Netzwerkgruppen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

Höchste Sicherheit

- Virtueller Arbeitsplatz garantiert die Sicherheit mobiler Daten
- Hardware- und Software-Verschlüsselung
- Zugriff auf zugelassene Anwendungen und Websites

Überragende Benutzerfreundlichkeit

- Sofortiger Plug-&-Play-Start
- Keine Software-Installation und kein Neustart erforderlich
- Zugriff von jedem Ort und jederzeit dank integrierter VPN-Funktion

Lösung mit geringsten Kosten

- Keine zusätzlichen Software-Lizenzen erforderlich
- Nutzt vorhandene Computer, VPN-Gateways und Managementsysteme
- Einfache Einrichtung und Verwaltung dank integriertem Management

Check Point GO

Sicherer virtueller Arbeitsplatz

SPEZIFIKATIONEN

Unterstützte Plattformen bei Check Point GO Host	
Betriebssysteme	• Windows 7 (32/64 Bit, Home Premium, Enterprise, Ultimate) • Windows Vista (32/64 Bit, Home und Professional, SP2+) • Windows XP (32 Bit, Home und Professional, SP3+)
Unterstützte Sprachen für Check Point GO Client	
Sprachen	• Englisch • Japanisch • Chinesisch (vereinfacht)
Verschlüsseltes USB-Laufwerk	
Betriebssysteme	• Windows 2000/2003, ME, XP, Vista • Solaris 8/9/10
SmartCenter Management Server	
Betriebssysteme	• Check Point SecurePlatform™ • Windows Server 2000/2003 • Solaris 8/9/10 • Red Hat Linux Enterprise 3.0
SmartCenter-GUI	
Betriebssysteme	• Windows 2000/2003, ME, XP, Vista • Solaris 8/9/10
Version R65	**Installiert mit:**
Security Gateway	• R65 HFA60 • R65 HFA60 Check Point GO Hotfix
SmartCenter Server	• R65 HFA60 • R65.4 oder R66 Check Point Connectra Plug-In • R65 HFA60 Check Point GO Hotfix
SmartDashboard Version	• R65.4 mit Check Point GO R70.1-Update
Version R70.20 oder R70.40	**Installiert mit:**
Security Gateway	Keine Ergänzungen
Security Management Server	Keine Ergänzungen
SmartDashboard Version	SmartDashboard für Versionen mit Check Point GO R70.1-Update
Version R71.1	**Installiert mit:**
Security Gateway	Keine Ergänzungen
Security Management Server	Keine Ergänzungen
SmartDashboard Version	R71.1 für Versionen mit Check Point GO R70.1-Update

Anwendungen, die im Check Point GO Secure Workspace auf Funktionstüchtigkeit getestet wurden		
• Adobe Acrobat (Writer) • Adobe Reader 8/9 • Citrix (Web- und Fat Clients, XenApp, NetScaler) • ClearQuest • CuteFTP • Cyberarc • Famatech Remote Administrator • FileZilla • Google Chrome Portable • iNotes	• Microsoft HyperTerminal • Microsoft Internet Explorer 6/7/8 • Microsoft Media Player • Microsoft Notepad • Microsoft Office XP/2003/2007 Excel, PowerPoint und Word • Microsoft Paint • Microsoft Terminal Services (RDP) Client (auch mstsc) • Microsoft Windows Image Viewer • Mozilla Firefox Version 3 und höher • Mozilla Firefox Portable Edition von http://portableapps.com • Mozilla Thunderbird Portable Edition von http://portableapps.com	• OpenOffice (Excel, PowerPoint und Word) • OpenOffice.org Portable Office Suite: Writer, Calc und Impress von http://portableapps.com • Outlook Web Access • Personal Communications Workstation Program • PowerTerm InterConnect für Windows • Putty • SecureCRT • Siebel Client • Sumatra PDF Portable PDF Reader von http://portableapps.com • VNC Viewer • WebDav • WinRar • WinZip • WordPadCalc • WS_FTP Home/PRO

Check Point
Services

Mit den Sicherheitsdiensten von Check Point stehen Ihnen umfassende technische Ressourcen und Support zur Verfügung, damit Sie Bedrohungen stets einen Schritt voraus sind. Dank der Support-Programme und -Pläne von Check Point können Sie bei Bedarf sofort auf wichtige Ressourcen zugreifen.

SmartDefense Services

Support-Programme und -Pläne von Check Point

Professional Services

Schulung und Zertifizierung

Check Point SmartUse

Support-Programme und -Pläne von Check Point

Flexible Support-Angebote für Ihre spezifischen Anforderungen

ÜBERSICHT

Check Point bietet zahlreiche Support-Optionen für seine Software- und Hardware-Sicherheitslösungen, die dank flexibler Rahmenbedingungen die speziellen Anforderungen eines jeden Unternehmens abdecken. Unabhängig davon, ob die Unterstützung direkt durch Check Point oder durch das globale Check Point-Netzwerk von Certified Collaborative Support Providern erfolgt – stets ist erstklassiger Support für alle Check Point-Produkte sichergestellt. Check Point Direct Enterprise Support bietet direkte Endkundenunterstützung, um Unternehmen bei der effizienten Bereitstellung, Konfiguration und Wartung von Check Point-Lösungen zu unterstützen. Collaborative Enterprise Support beinhaltet die First-Line-Unterstützung durch einen lokalen Certified Collaborative Support Provider, der seinerseits auf umfassende Back-End-Unterstützung durch die Check Point Technical Assistance Center zurückgreifen kann. Der Check Point Appliance Support bietet Upgrade-, Reparatur- und Austauschdienstleistungen für Check Point-Hardware.

VORTEILE

- Flexible Rahmenbedingungen und Service Level Agreements (SLAs) erfüllen eine breite Palette verschiedener Bedürfnisse
- Abgestufte Reparaturdienstleistungen schützen die Investitionen des Unternehmens in Check Point-Lösungen durch passende Support-Programme für Ihre Anforderungen
- Rund um die Uhr in ständiger Bereitschaft stehender Support mit ausgefeilten Methoden, Prozessen und Tools zur Koordinierung der kontinuierlichen Abdeckung
- Auswahl zwischen direkter Unterstützung durch Check Point und Unterstützung durch das integrierte globale Netzwerk von Certified Collaborative Support Providern
- Schnelle Lieferung von Hardware-Ersatzteilen garantiert vor 9:00 Uhr des nächsten Tages (in den meisten Gebieten)

LEISTUNGSMERKMALE

- Check Point Enterprise Based Support (EBS) bietet direkten Endkundensupport inklusive technischer Unterstützung per Telefon, Internet und Chat und berechtigt darüber hinaus zum Zugriff auf das Check Point Support Center für Hilfe zu einem beliebigen Zeitpunkt
- Check Point Collaborative Enterprise Support (CES) bietet First-Line-Unterstützung durch einen lokalen Certified Collaborative Support Provider (CCSP), der Support-Dienstleistungen in der lokalen Sprache des Kunden erbringt und über genaue Kenntnis der Kundenumgebung verfügt sowie zusätzlich durch Check Point-Experten unterstützt wird
- Der Check Point Appliance Support bietet technische Unterstützung für sämtliche Hardware- und Software-Updates und -Upgrades sowie für den Austausch fehlerhafter Hardware
- Das Check Point Support Center ist ein individuell angepasstes Support-Portal, das sicheren Zugriff auf umfassende Online-Lösungen zur Selbsthilfe in Echtzeit bietet – wann immer und wo immer diese benötigt wird

INTERESSANT FÜR

- Alle Kunden, die ihre Investitionen in Hardware- oder Software-Sicherheitslösungen von Check Point schützen wollen
- Alle Check Point-Kunden, die sicherstellen wollen, dass ihre wertvollen IT-Assets kontinuierlich aktualisiert werden und stets geschützt sind, um maximale Sicherheit, Konnektivität und Zuverlässigkeit zu garantieren

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Bietet lokale persönliche Unterstützung durch ein globales Netzwerk zertifizierter Check Point Collaborative Support-Partner, welche über genaue Kenntnis der Kundenumgebung verfügen und First-Line-Support in der lokalen Kundensprache erbringen
- Stellt durch nahtlose Integration lokaler Support Provider und ein globales Netzwerk von Check Point Technical Assistance Centern (TAC) sicher, dass Probleme schnell an den richtigen Ansprechpartner verwiesen werden. Auf diese Weise werden kostspielige Verzögerungen vermieden, die durch mehrfache Übergaben und die Wiederholung von Informationen entstehen

GESPRÄCHSEINSTIEG

- Wünschen Sie direkten Zugang zu einer umfangreichen Online-Knowledgebase mit Lösungen zur Selbsthilfe, mittels derer Ihre Fragen schnell und einfach beantwortet sowie Support-Zeitaufwand und -Kosten reduziert werden?
- Würden Sie einen Vorteil daraus ziehen, wenn Ihnen ein lokaler Experte mit genauen Kenntnisse über Ihre Umgebung zur Seite stünde?
- Wünschen Sie webbasierten Zugang zu einem zuverlässigen Support-Portal, das rund um die Uhr Unterstützung bietet?
- Sind Sie an einem Programm interessiert, das technische Unterstützung, Software-Updates und -Upgrades sowie den Austausch fehlerhafter Hardware umfasst?
- Würden Sie im Falle von Hardware-Fehlern von einem Programm profitieren, das den Austausch der fehlerhaften Hardware bis 9:00 Uhr des nächsten Arbeitstages garantiert?

Support-Programme und -Pläne von Check Point

Flexible Support-Angebote für Ihre spezifischen Anforderungen

CHECK POINT ENTERPRISE SUPPORT

Check Point Enterprise Support-Programme bieten eine umfassende Palette an Funktionen und Vorteilen. Dabei können Sie zwischen verschiedenen Service Leveln wählen.

Support-Service	Software Subscription	Standard	Premium	Elite	Diamond zusätzlich zu Premium oder Elite)
Basis-SLA	n. v.	5 x 9, werktags	7 x 24, täglich	7 x 24, täglich	7 x 24, täglich
Check Point-Techniker vor Ort bei kritischen Serviceanforderungen	Nein	Nein	Nein	Ja**	Hängt von der Support-Stufe ab
TAC-Zugang					
Ansprechpartner im Support	n. v.	Desks Support Engineer	Premium Support Engineer	Premium Support Engineer	Spezieller Diamond Engineer
Unbegrenzte Serviceanforderungen	n. v.	Ja	Ja	Ja	Ja
Garantierte Reaktionszeit bei Problemen mit Severity Level 1*	n. v.	30 Minuten	30 Minuten	30 Minuten	30 Minuten
Garantierte Reaktionszeit bei Problemen mit Severity Level 2, 3 und 4*	n. v.	4 Stunden	Severity Level 2: 2 Stunden	Severity Level 2: 30 Minuten	Hängt von der Support-Stufe ab
			Severity Level 3 und 4: 4 Stunden	Severity Level 3 und 4: 4 Stunden	Severity Level 3 und 4: 4 Stunden
Support-Tools					
Neueste Hotfixes und Service Packs	Ja	Ja	Ja	Ja	Ja
Wichtige Upgrades & Verbesserungen	Ja	Ja	Ja	Ja	Ja
Zugang zu den Produkt-foren von Check Point	Lesen	Vollständiger Zugang	Vollständiger Zugang	Vollständiger Zugang	Vollständiger Zugang
Zugang zur Online-Support-Knowledgebase	n. v.	Advanced	Expert	Expert	Expert
Appliance-Support					
Standard-Appliance-Support (wenn die Appliance Bestandteil der Account Rate ist)	1 Jahr Garantie	Standard	Premium	Elite	Hängt von der Support-Stufe ab
Return Materials Authorization (RMA)-Ermittlung	TAC	TAC	TAC	TAC	Kunde
RMA-Versandmethode	Innerhalb von 7 Werktagen nach Rückgabe der defekten Einheit	Versand am gleichen Werktag[1]	Nächster Flug/ Expressversand (wenn zutreffend) oder Versand am gleichen Werktag[3]	Nächster Flug/ Expressversand (wenn zutreffend) oder Versand am gleichen Werktag[3]	Nächster Flug/ Expressversand (wenn zutreffend) oder Versand am gleichen Werktag[3]
Vor-Ort-RMA-Versandmethode (muss zusätzlich zum regulären SLA des Programms gekauft werden)	n. v.	5 x 8 x nächster Werktag Lieferung und grundlegende Installation der Ersatz-Hardware durch einen zertifi-zierten Techniker[2]	7 x 24 x 4 Stunden Lieferung und grundlegende Installation der Ersatz-Hardware durch einen zertifi-zierten Techniker[2]	7 x 24 x 4 Stunden Lieferung und grundlegende Installation der Ersatz-Hardware durch einen zertifi-zierten Techniker2	7 x 24 x 4 Stunden Lieferung und grundlegende Installation der Ersatz-Hardware durch einen zertifi-zierten Techniker[2]

[1] Bei abgeschlossener RMA bis 15.00 Uhr (Zeit am regionalen Hub); ansonsten erfolgt der Versand am nächsten Werktag (mit Anlieferung am nächsten Tag).
[2] Verfügbar an über 250 Standorten weltweit.
[3] Nächster Flug/Expressversand in der EU und in den USA (Festland) verfügbar. Appliances werden während der regulären Geschäftszeiten versandt und können außerhalb der Geschäftszeiten ankommen.
* Bei einem SLA mit 30 Minuten wird eine Echtzeitkommunikation (Chat, Telefon) benötigt
** SLA mit CP-Techniker vor Ort: Entsendung eines Notfalltechnikers bei kritischen Problemen innerhalb von 4 Stunden nach Öffnung des Tickets (kritisches Problem: Severity Level 1 – Netzwerkausfall, der eine 7x24-Behebung durch Kunden, Partner und Check Point erforderlich macht); siehe Definition

Support-Programme und -Pläne von Check Point

Flexible Support-Angebote für Ihre spezifischen Anforderungen

PERSONALISIERTER SUPPORT

Erweitern Sie den Enterprise Premium- und Elite-Support mit personalisierten Diamond/Diamond PLUS-Programmen – inklusive eines dedizierten Technikers, einer individuellen Supportnummer, umfassender Ressourcen, Beratung und vielem mehr.

Wählen Sie die **Collaborative Enterprise Support**-Stufe und Back-Line-Support anhand Ihrer Anforderungen aus:

Support-Service	Co-Standard	Co-Premium	Co-Elite
SLA-Anpassung bei Endkunden	5 x 9, werktags	7 x 24, täglich	7 x 24, täglich
Unbegrenzter TAC-Zugang für zertifizierten Support-Partner	7 x 24, täglich	7 x 24, täglich	7 x 24, täglich
Check Point-Techniker vor Ort bei kritischen Serviceanforderungen	Nein	Nein	Ja**
TAC-Zugang			
Ansprechpartner im Support	Desks Support Engineer	Premium Support Engineer	Premium Support Engineer
Garantierte Reaktionszeit bei Problemen mit Severity Level 1*	30 Minuten	30 Minuten	30 Minuten
Garantierte Reaktionszeit bei Problemen mit Severity Level 2, 3 und 4*	4 Stunden	Severity Level 2: 2 Stunden	Severity Level 2: 30 Minuten
		Severity Level 3 und 4: 4 Stunden	Severity Level 3 und 4: 4 Stunden
Support-Tools			
Neueste Hotfixes und Service Packs	Ja	Ja	Ja
Wichtige Upgrades & Verbesserungen	Ja	Ja	Ja
Zugang zu den Produktforen von Check Point	Vollständiger Zugang	Vollständiger Zugang	Vollständiger Zugang
Zugang zur Online-Support-Knowledgebase	Advanced	Expert	Expert
Appliance-Support			
Standard-Appliance-Support (wenn die Appliance Bestandteil der Account Rate ist)	Co-Standard	Co-Premium	Co-Elite
Return Materials Authorization (RMA)-Ermittlung	TAC	Partner***	Partner***
RMA-Versandmethode	Versand am gleichen Werktag[1]	Nächster Flug/ Expressversand (wenn zutreffend) oder Versand am gleichen Werktag[3]	Nächster Flug/ Expressversand (wenn zutreffend) oder Versand am gleichen Werktag[3]
Vor-Ort-RMA-Versandmethode (muss zusätzlich zum regulären SLA des Programms gekauft werden)	5 x 8 x nächster Werktag Lieferung und grundlegende Installation der Ersatz-Hardware durch einen zertifizierten Techniker	7 x 24 x 4 Stunden Lieferung und grundlegende Installation der Ersatz-Hardware durch einen zertifizierten Techniker[2]	7 x 24 x 4 Stunden Lieferung und grundlegende Installation der Ersatz-Hardware durch einen zertifizierten Techniker[2]

[1] Bei abgeschlossener RMA bis 15.00 Uhr (Zeit am regionalen Hub); ansonsten erfolgt der Versand am nächsten Werktag (mit Lieferziel ein Tag später).
[2] Verfügbar an über 250 Standorten weltweit.
[3] Nächster Flug/Expressversand in der EU und in den USA (Festland) verfügbar. Appliances werden während der regulären Geschäftszeiten versandt und können außerhalb der Geschäftszeiten ankommen.
* Bei einem SLA mit 30 Minuten wird Echtzeitkommunikation (Chat, Telefon) benötigt
** SLA mit CP-Techniker vor Ort: Entsendung eines Notfalltechnikers bei kritischen Problemen innerhalb von 4 Stunden nach Öffnung des Falls (kritisches Problem: Severity Level 1 – Netzwerkausfall, der eine 7x24-Behebung durch Kunden, Partner und Check Point erforderlich macht); siehe Definition
*** RMA-Genehmigungsnachweis setzt eine volle User Center Account Abdeckung mit Co-Premium/Co-Elite-SLA voraus, Appliance-Schulung; jährliche RMA-Rate von unter 7,5 % und eine False-Positive-Rate von unter 25 % voraus. Partner sind nicht dazu berechtigt, RMAs für IAS-Appliances zu genehmigen.

Support-Programme und -Pläne von Check Point

Flexible Support-Angebote für Ihre spezifischen Anforderungen

SUPPORT-PROGRAMME UND -PLÄNE

Dank der Support-Programme und -Pläne von Check Point können Sie bei Bedarf sofort auf wichtige Ressourcen zugreifen.

DIRECT ENTERPRISE SUPPORT

Direct Enterprise Support von Check Point bietet alle Vorteile einer Software Subscription mit umfassendem, unbegrenztem Support durch Check Points erfahrene und zertifizierte Sicherheitsexperten.

Wert der installierten Basis (SW)	Enterprise Software	Standard	Premium	Elite
< 50.000 USD	15,0 %	30,0 %	40,0 %	43,0 %
50.000 bis 100.000 USD	14,5 %	28,0 %	36,0 %	39,0 %
100.001 bis 250.000 USD	14,0 %	26,0 %	33,0 %	36,0 %
250.001 bis 500.000 USD	13,5 %	24,0 %	30,0 %	33,0 %
500.001 bis 1 Million USD	13,0 %	22,0 %	27,0 %	30,0 %
Über 1 Million USD	12,5 %	20,0 %	24,0 %	27,0 %

* Verfügbar in Nordamerika und anderen ausgewählten Regionen

COLLABORATIVE ENTERPRISE SUPPORT*

Collaborative Enterprise Support von Check Point umfasst First-Line-Support von Ihrem lokalen Certified Collaborative Support Provider (CCSP) sowie vollständigen Back-End-Support von Check Point.

Wert der installierten Basis (SW)	Co-Standard	Co-Premium	Co-Elite**
< 50.000 USD	18,0 %	24,0 %	27,0 %
50.000 bis 100.000 USD	17,5 %	23,5 %	26,5 %
100.001 bis 250.000 USD	17,0 %	23,0 %	26,0 %
250.001 bis 500.000 USD	16,6 %	22,5 %	25,0 %
500.001 bis 1 Million USD	16,0 %	22,0 %	25,0 %
Über 1 Million USD	15,5 %	21,5 %	24,5 %

* Verfügbar in EMEA, APAC, Lateinamerika und anderen ausgewählten Regionen
** Entsendung von Notfalltechnikern bei kritischen Software-Problemen

Hinweis:
Der oben aufgeführte Preis für Collaborative Enterprise Support gilt ausschließlich für Back-Line-Support von Check Point.

Support-Programme und -Pläne von Check Point

Flexible Support-Angebote für Ihre spezifischen Anforderungen

DIRECT ENTERPRISE SUPPORT

Direct Enterprise Support von Check Point bietet alle Vorteile einer Software Subscription mit umfassendem, unbegrenztem Support durch Check Points erfahrene und zertifizierte Sicherheitsexperten.

Name des Programms	Wert der installierten Basis	Artikelnummer	Listenpreis	Zusätzliche telefonische Beratung (0,5 Tag) CPTS-PRO-SPRT-4HR	Zusätzliche Beratung vor Ort (1 Tag) CPTS-PRO-CON-DAILY
Diamond III	< 500.000 USD	CPES-SS-DIAMOND 3	50.000 USD	700 USD	2.250 USD
Diamond III PLUS		CPES-SS-DIAMOND 3 PLUS	100.000 USD		
Diamond II	500.001 bis 1 Million USD	CPES-SS-DIAMOND 2	75.000 USD	700 USD	2.100 USD
Diamond II PLUS		CPES-SS-DIAMOND 2 PLUS	150.000 USD		
Diamond I	Über 1 Million USD	CPES-SS-DIAMOND 1	100.000 USD	700 USD	2.000 USD
Diamond I PLUS		CPES-SS-DIAMOND 1 PLUS	200.000 USD		
Zusätzliche TAM-Beratung	Beliebig	CPTS-PRO-ADD-ATAM	30.000 USD		

Hinweis: Diamond PLUS bietet branchenführende Supportdienstleistungen inklusive Advanced Technical Account Management (TAM). Advanced TAM erweitert die TAC-Services um Designprüfungen, proaktives Kundenmanagement, Betriebsunterstützung und Hilfe durch Testlabore. So erhalten Sie eine umfassende proaktive und reaktive Lösung. Besuchen Sie die Advanced TAM-Seite, um mehr Informationen zu erhalten.
Das Diamond PLUS Add-On beinhaltet bis zu 25 Beratungstage (bis zu 15 Tage vor Ort, TE eingeschlossen)

APPLIANCE-SUPPORT

Check Point Appliance-Support ist eine umfassende Lösung für HW- und SW-Support (inklusive Diagnose, Fehlerbehebung und ggf. Austausch von Teilen/Geräten). Dabei werden SLAs angewendet, die den Support-Programmen von Check Point entsprechen.

DIRECT APPLIANCE SUPPORT (EBS)

Produktpalette	Standard	Standard-RMA Nächster Werktag vor Ort**	Premium*	Premium-RMA, 4 Stunden vor Ort**	Elite***	Elite-RMA, 4 Stunden vor Ort**
	CPES-SS-STANDARD Jährliche Support-Rate	CPES-SS-STANDARD-ONSITE	CPES-SS-PREMIUM Jährliche Support-Rate	CPES-SS-PREMIUM-ONSITE	20 %	26 %
High End	12 %	20 %	17 %	23 %	20 %	28 %
Mid Range	12 %	22 %	17 %	25 %	20 %	33 %
Low End	12 %	27 %	17 %	30 %	Elite-Kundenrate	Elite-Kundenrate + 8 %
2 Blade Appliance xx2 Serie (wie UTM-1 272,572 oder NGX, nicht Total Security)	Standard-Kundenrate	Standard-Kundenrate + 10 %	Premium-Kundenrate	Premium-Kundenrate + 8 %	27,0 %	30,0 %

* Nächster Flug/Expressversand in der EU und in den USA (Festland) verfügbar. Appliances werden während der regulären Geschäftszeiten versandt und können außerhalb der Geschäftszeiten oder am nächsten Werktag vor 9.00 Uhr ankommen.
** Von Check Point zertifizierte Techniker stellen weltweit Vor-Ort-Services bereit.
*** Entsendung von Notfalltechnikern bei kritischen Software-Problemen

Hinweis:
- Vor-Ort-Hardware-Support ist erst einen (1) Monat nach dem Kaufdatum verfügbar.
- Auf alle anderen Check Point-Appliances, die nicht in der Appliance-Klassifizierungstabelle aufgeführt sind, wird die reguläre Account Rate angewendet. Ein Vor-Ort-Service ist nicht verfügbar.
- Kunden können anhand ihrer betrieblichen Anforderungen Support-Upgrades für einzelne Appliances kaufen (unabhängig vom User Account Service Level Agreement des Kunden).

Support-Programme und -Pläne von Check Point

Flexible Support-Angebote für Ihre spezifischen Anforderungen

COLLABORATIVE APPLIANCE SUPPORT (CES)

Gültigkeit weltweit (ausgenommen USA und Kanada)

Produktpalette	Co-Standard	Co-Standard-RMA Nächster Werktag vor Ort**	Co-Premium*	Co-Premium-RMA, 4 Stunden vor Ort**	Co-Elite***	Co-Elite-RMA, 4 Stunden vor Ort**
	CPES-CO-STANDARD Jährliche Account-Rate	CPES-CO-STANDARD-ONSITE Jährliche Account-Rate	CPES-CO-PREMIUM Jährliche Account-Rate	CPES-CO-PREMIUM-ONSITE Jährliche Account-Rate	CPES-CO-ELITE Jährliche Account-Rate	CPES-CO-ELITE-ONSITE Jährliche Account-Rate
High End	10 %	17 %	15 %	20 %	18 %	23 %
Mid Range	10 %	19 %	15 %	22 %	18 %	25 %
Low End	10 %	24 %	15 %	27 %	18 %	30 %
2 Blade appliance xx2 series (like UTM-1 272,572 or NGX non Total Security)	Co-Standard-Kundenrate	Co-Standard-Account Rate + 9 %	Co-Premium-Account Rate	Co-Premium-Account Rate + 7 %	Co-Elite-Account Rate	Co-Elite-Account Rate + 7 %

* Nächster Flug/Expressversand in der EU und in den USA (Festland) verfügbar. Appliances werden während der regulären Geschäftszeiten versandt und können außerhalb der Geschäftszeiten oder am nächsten Werktag vor 9.00 Uhr ankommen.
** Von Check Point zertifizierte Techniker stellen weltweit Vor-Ort-Services bereit.
*** Entsendung von Notfalltechnikern bei kritischen Software-Problemen

Hinweis:
- Vor-Ort-Hardware-Support ist erst einen (1) Monat nach dem Kaufdatum verfügbar.
- Auf alle anderen Check Point-Appliances, die nicht in der Appliance-Klassifizierungstabelle aufgeführt sind, wird die reguläre Account Rate angewendet. Ein Vor-Ort-Service ist nicht verfügbar.
- Kunden können anhand ihrer betrieblichen Anforderungen Support-Upgrades für einzelne Appliances kaufen (unabhängig vom User Account Service Level Agreement des Kunden)
- Der oben aufgeführte Preis für Collaborative Appliance Support gilt ausschließlich für Back-Line-Support von Check Point.

Support-Programme und -Pläne von Check Point

Flexible Support-Angebote für Ihre spezifischen Anforderungen

APPLIANCE-KLASSIFIZIERUNG

Appliance-Palette	Security Gateway Appliances	Smart-1	VSX-1	Dedizierte Gateways
High End	12400 Appliances 12600 Appliances 21x00 Appliances 61000 Appliances Power-1 5075 / 5077 Power-1 9075 / 9077 Power-1 11xxx Serie IP 1285 / 1287 IP 2455 / 2457	Smart-1 50 Smart-1 150	VSX 12400 VSX 12600 VSX 21400 VSX-1 3070 VSX-1 9070 VSX-1 9090 VSX-1 11xxx Serie VSX-1 112xx Serie	DLP-1 9571 IPS-1 9070 IPS-1 5070 Connectra 9072
Mid Range	4400 Appliances 4600 Appliances 4800 Appliances 12200 Appliances UTM-1 274 / 276 / 278 UTM-1 574 / 576 / 578 UTM-1 1073 / 1075 / 1076 / 1078 UTM-1 2073 / 2075 / 2076 / 2078 UTM-1 3073 / 3075 / 3076 / 3078 IP 295 / 297 IP 395 / 397 IP 565 / 567 IP 695 / 697	Smart-1 5 Smart-1 25	VSX 12200	DLP-1 2571 IPS-1 2070 IPS-1 4070 Connectra 270 Connectra 3070
Low End	2200 Appliances 4200 Appliances UTM-1 134 / 136 / 138 SG86*			

* Vor-Ort-Services für SG82 & SG86 umfassen lediglich den Produktaustausch (ohne Techniker).

- Die oben aufgeführten speziellen Account Rates gelten ausschließlich für auf Software Blades basierende Appliances mit drei Blades (und mehr) sowie NGX-basierte UTM-1 Total Security- und Power-1-Appliances.
- Bei NGX UTM-1-Appliances (nicht Total Security) wird die reguläre Account Rate angewendet. UTM-1 Edge-RMA wird bei allen SLAs am nächsten Werktag versandt.
- Auf alle anderen Check Point-Appliances, die nicht in der Tabelle oben aufgeführt sind (z. B. UTM-1 Edge), werden die regulären Account Rates angewendet. Außerdem sind keine Vor-Ort-Services verfügbar (mit Ausnahme von 2-Blade-Appliances und NGX ohne Total Security).
- Für die UTM-1 xx50 Serie können Sie ausschließlich Premium-/Standard-/Elite-Support kaufen. Vor-Ort-Services sind nicht verfügbar (es sei denn, es handelt es sich um eine Vor-Ort-Verlängerung).

ENDPOINT SECURITY – CHECK POINT GO SUPPORT

Produkt	Collaborative Appliance Support (CES)	
	Co-Standard CPCES-CO-STANDARD CAT-Support	Co-Premium CPCES-CO-PREMIUM CAT-Support
Check Point GO USB-Stick	10 %	15 %
	Direct Appliance Support (EBS)	
	Standard CPES-SS-STANDARD CAT-Support	Premium CPES-SS-PREMIUM CAT-Support
Check Point GO USB-Stick	12 %	17 %

Check Point Support Timeline

Aktuelle Infos finden Sie jederzeit unter: http://www.checkpoint.com/services/lifecycle/appliance-support.html

CHECK POINT APPLIANCE SUPPORT TIMELINE

Appliance Product/ Model	Status	General Availability	Appliance Being Replaced	Successor Product Availability Date	End of Engineering Support	End of Support*	Latest Available Software Version
2012 Appliances							
2200 Appliance	Active	October 2011	UTM-1 130				R75, R71, & current HFAs
4200 Appliance	Active	October, 2011	IP150, UTM-1 270				R75, R71, & current HFAs
4400 Appliance	Active	May, 2012	UTM-1 570				R75, R71, & current HFAs
4600 Appliance	Active	October, 2011	UTM-1 1070				R75, R71, & current HFAs
4800 Appliance	Active	October, 2011	UTM-1 2070				R75, R71, & current HFAs
12200 Appliance	Active	October, 2011	UTM-1 3070				R75, R71, & current HFAs
12400 Appliance	Active	October, 2011	Power-1 5070				R75, R71, & current HFAs
12600 Appliance	Active	October, 2011	Power-1 9070				R75, R71, & current HFAs
High End Data Center Appliances							
21400 Appliance	Active	August, 2011	Power-1 11000				R75, R71, & current HFAs
61000 Appliance	Active	August, 2011	None				R75
Series 80							
Model 80	Active	August, 2010	None				R71
Smart-1							
Smart-1 5	Active	June, 2009	None				R70, R71, R75 & current HFAs
Smart-1 25	Active	June, 2009	None				R70, R71, R75 & current HFAs
Smart-1 50	Active	June, 2009	None				R70, R71, R75 & current HFAs
Smart-1 150	Active	June, 2009	None				R70, R71, R75 & current HFAs
Safe@Office							
Safe@ 500	Successor Product Available	NA	None	31-May-2010	31-May-2013	31-May-2015	8.1
Safe@ 1000	Active	May 2010	Safe@ 500				8.1

Check Point Support Timeline

Aktuelle Infos finden Sie jederzeit unter: http://www.checkpoint.com/services/lifecycle/appliance-support.html

CHECK POINT APPLIANCE SUPPORT TIMELINE

Appliance Product/ Model	Status	General Availability	Appliance Being Replaced	Successor Product Availability Date	End of Engineering Support	End of Support*	Latest Available Software Version
UTM-1							
UTM-1 Edge X	Successor Product Available	NA	None	31-May-2010	31-May-2013	31-May-2015	8.1
UTM-1 Edge N	Active	May 2010	UTM-1 Edge X				8.1
UTM-1 Edge Industrial	Successor Product Available		None	1-May-2012	1-May-2015	1-May-2017	8.1
UTM-1 Edge N Industrial	Active	May, 2012	UTM-1 Edge Industrial				
UTM-1 130	Successor Product Available	February, 2009	None	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
UTM-1 270	Successor Product Available	April, 2008	None	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
UTM-1 570	Successor Product Available	April, 2008	UTM-1 450	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
UTM-1 1070	Successor Product Available	July, 2008	UTM-1 1050	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
UTM-1 2070	Successor Product Available	July, 2008	UTM-1 2050	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
UTM-1 3070	Successor Product Available	April, 2008	None	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
UTM-1 450	Successor Product Available	February, 2007	None	1-Oct-2008	1-Oct-2011	1-Oct-2013	R70, R71 & current HFAs
UTM-1 1050	Successor Product Available	February, 2007	None	1-Oct-2008	1-Oct-2011	1-Oct-2013	R70, R71 & current HFAs
UTM-1 2050	Successor Product Available	February, 2007	None	1-Oct-2008	1-Oct-2011	1-Oct-2013	R70, R71 & current HFAs
Power-1							
Power-1 5070	Successor Product Available	April, 2008	None	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
Power-1 9070	Successor Product Available	April, 2008	None	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
Power-1 11060	Successor Product Available	April, 2009	None	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
Power-1 11070	Successor Product Available	April, 2009	None	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs
Power-1 11080	Successor Product Available	April, 2009	None	1-April-2012	1-April-2015	1-April-2017	R70, R71, R75 & current HFAs

Check Point Support Timeline

Aktuelle Infos finden Sie jederzeit unter: http://www.checkpoint.com/services/lifecycle/appliance-support.html

CHECK POINT APPLIANCE SUPPORT TIMELINE

Appliance Product/ Model	Status	General Availability	Appliance Being Replaced	Successor Product Availability Date	End of Engineering Support	End of Support*	Latest Available Software Version
IP Appliances							
IP150	Successor, Product, Available	May, 2008	IP110/ IP120/ IP130	1-Jan-2012	1-Jan-2015	1-Jan-2017	6.2; R70, R71, R75 & current HFAs
IP280	Active	July, 2010	IP150			At least until 2016	6.2; R70, R71, R75 & current HFAs
IP290	Active	March, 2007	IP260/ IP265			At least until 2016	6.2; R70, R71, R75 & current HFAs
IP390	Active	May, 2006	IP35X/ IP38X			At least until 2016	6.2; R70, R71, R75 & current HFAs
IP560	Active	February, 2006	IP530			At least until 2016	6.2; R70, R71, R75 & current HFAs
IP690	Active	May, 2007	IP650			At least until 2016	6.2; R70, R71, R75 & current HFAs
IP1280	Active	April, 2008	IP1220/ IP1260			At least until 2016	6.2; R70, R71, R75 & current HFAs
IP2450	Active	August, 2007	IP2250/ IP2255			At least until 2016	6.2; R70, R71, R75 & current HFAs
IP45	Successor, Product, Available	June, 2006	NA	30-Jun-2007	30-Jun-2009	30-Jun-2009	4
IP60	Successor, Product, Available	November, 2006	NA	1-Jul-2009	1-Jul-2012	1-Jul-2012	8
IP130	Successor, Product, Available	June, 2003	NA	31-Dec-2005	31-Dec-2008	31-Dec-2010	4.2; R62
IP260	Successor, Product, Available	January, 2005	NA	30-Jun-2008	30-Jun-2011	30-Jun-2013	4.2; R65
IP265	Successor, Product, Available	December, 2004	NA	31-Dec-2007	31-Dec-2010	31-Dec-2012	4.2; R62
IP350	Successor, Product, Available	June, 2002	NA	30-Nov-2006	30-Nov-2011	30-Nov-2011	4.2; R65
IP355	Successor, Product, Available	June, 2002	NA	30-Nov-2006	30-Nov-2011	30-Nov-2011	4.2; R65
IP380	Successor, Product, Available	June, 2002	NA	30-Nov-2006	30-Nov-2011	30-Nov-2011	4.2; R65
IP385	Successor, Product, Available	June, 2002	NA	30-Nov-2006	30-Nov-2011	30-Nov-2011	4.2; R65
IP530	Successor, Product, Available	March, 2001	NA	31-Mar-2005	31-Mar-2010	31-Mar-2010	4.2; R62
IP710	Successor, Product, Available	May, 2002	NA	30-Apr-2006	30-Apr-2011	30-Apr-2011	4.2; R65
IP740	Successor, Product, Available	July, 2001	NA	30-Jun-2005	30-Jun-2010	30-Jun-2010	4.2; R65
IP1220	Successor, Product, Available	April, 2004	NA	31-Dec-2008	31-Dec-2011	31-Dec-2013	4.2; R65
IP1260	Successor, Product, Available	June, 2003	NA	31-Dec-2008	31-Dec-2011	31-Dec-2013	4.2; R65
IP2250	Successor, Product, Available	April, 2004	NA	31-May-2006	31-Dec-2011	31-Dec-2013	4.2; R65
IP2255	Successor, Product, Available	July, 2006	NA	31-Dec-2008	31-Dec-2011	31-Dec-2013	4.2; R65
12400 Appliance	Active	October, 2011	Power-1 5070				R75, R71, & current HFAs

Check Point Support Timeline

Aktuelle Infos finden Sie jederzeit unter: http://www.checkpoint.com/services/lifecycle/appliance-support.html

CHECK POINT APPLIANCE SUPPORT TIMELINE

Appliance Product/ Model	Status	General Availability	Appliance Being Replaced	Successor Product Availability Date	End of Engineering Support	End of Support*	Latest Available Software Version
IAS M series							
IAS M2	Active	June, 2008	None				R70, R71, R75 & current HFAs
IAS M6	Active	June, 2008	None				R70, R71, R75 & current HFAs
IAS M8	Active	June, 2008	None				R70, R71, R75 & current HFAs
VSX Appliances							
12200 VSX	Active	October, 2011	VSX-1 3070				NGX R67 VSX & current HFAs
12400 VSX	Active	October, 2011	VSX-1 9070, VSX-1 9090				NGX R67 VSX & current HFAs
12600 VSX	Active	October, 2011	VSX-1 9070, VSX-1 9090				NGX R67 VSX & current HFAs
21400 VSX	Active	August, 2011	VSX-1 11285, VSX-1 11085, VSX-1 11275, VSX-1 11075, VSX-1 11265, VSX-1 11065				NGX R67 VSX & current HFAs
VSX-1 11285	Successor Product Available	June, 2010	None	1-April-2012	1-April-2015	1-April-2017	NGX R68, NGX R67 VSX & current HFAs
VSX-1 11085	Successor Product Available	June, 2010	None	1-April-2012	1-April-2015	1-April-2017	NGX R68, NGX R67 VSX & current HFAs
VSX-1 11275	Successor Product Available	June, 2010	None	1-April-2012	1-April-2015	1-April-2017	NGX R68, NGX R67 VSX & current HFAs
VSX-1 11075	Successor Product Available	June, 2010	None	1-April-2012	1-April-2015	1-April-2017	NGX R68, NGX R67 VSX & current HFAs
VSX-1 11265	Successor Product Available	June, 2010	None	1-April-2012	1-April-2015	1-April-2017	NGX R68, NGX R67 VSX & current HFAs
VSX-1 11065	Successor Product Available	June, 2010	None	1-April-2012	1-April-2015	1-April-2017	NGX R68, NGX R67 VSX & current HFAs
VSX-1 9090	Successor Product Available	February, 2009	None	1-April-2012	1-April-2015	1-April-2017	NGX R68 VSX, NGX R67 VSX, NGX R65 VSX & current HFAs
VSX-1 9070	Successor Product Available	February, 2009	None	1-April-2012	1-April-2015	1-April-2017	NGX R68 VSX, NGX R67 VSX, NGX R65 VSX & current HFAs
VSX-1 3070	Successor Product Available	February, 2009	None	1-April-2012	1-April-2015	1-April-2017	NGX R68 VSX, NGX R67 VSX, NGX R65 VSX & current HFAs

Check Point Support Timeline

Aktuelle Infos finden Sie jederzeit unter: http://www.checkpoint.com/services/lifecycle/appliance-support.html

CHECK POINT APPLIANCE SUPPORT TIMELINE

Appliance Product/ Model	Status	General Availability	Appliance Being Replaced	Successor Product Availability Date	End of Engineering Support	End of Support*	Latest Available Software Version
Connectra							
Connectra 270	Successor Product Available	October, 2008	Connectra 1000	1-Oct-2011	1-Jan-2015	1-Jan-2017	NGX R66
Connectra 3070	Successor Product Available	October, 2008	Connectra 2000	1-Oct-2011	1-Jan-2015	1-Jan-2017	NGX R66
Connectra 9072	Successor Product Available	October, 2008	Connectra 6000	1-Oct-2011	1-Jan-2015	1-Jan-2017	NGX R66
Connectra 1000	Successor Product Available	May-2004	NA	1-Oct-2008	1-Oct-2011	1-Oct-2011	NGX R66
Connectra 2000	Successor Product Available	May-2004	NA	1-Oct-2008	1-Oct-2011	1-Oct-2011	NGX R66
Connectra 6000	Successor Product Available	May-2004	NA	1-Oct-2008	1-Oct-2011	1-Oct-2011	NGX R66
IPS-1							
IPS-1 2070	Active	August, 2010	Sensor 50	None			R71
IPS-1 4070	Active	August, 2010	Sensor 200	None			R71
IPS-1 5070	Active	August, 2010	Sensor 500	None			R71
IPS-1 9070	Active	August, 2010	Power Sensor 1000	None			R71
IPS-1 IAS Solutions	Active	August, 2010	Power Sensor 2000	None			R71
Sensor 50	Successor Product Available	September, 2006	Sensor 20	August, 2010	August, 2013	August, 2015	R71
Sensor 200	Successor Product Available	June, 2005	Sensor 100	August, 2010	August, 2013	August, 2015	R71
Sensor 500	Successor Product Available	June, 2005	None	August, 2010	August, 2013	August, 2015	R71
Power Sensor 1000	Successor Product Available	November, 2005	None	August, 2010	March, 2013	March, 2013	R65.2
Power Sensor 2000	Successor Product Available	November, 2005	None	August, 2010	March, 2013	March, 2013	R65.2
Sensor 20	Successor Product Available	September, 2006	None	March, 2007	March, 2010	March, 2012	5.0.6
Sensor 100	Successor Product Available	June, 2005	None	March, 2007	March, 2010	March, 2012	5.0.6

Check Point Support Timeline

Aktuelle Infos finden Sie jederzeit unter: http://www.checkpoint.com/services/lifecycle/appliance-support.html

CHECK POINT APPLIANCE SUPPORT TIMELINE

Appliance Product/ Model	Status	General Availability	Appliance Being Replaced	Successor Product Availability Date	End of Engineering Support	End of Support*	Latest Available Software Version
IP VPN Platforms							
5i	Successor Product Available	June, 2006	NA	1-Jul-2009	1-Jul-2012	1-Jul-2014	6.3.3
10i	Successor Product Available	June, 2006	NA	1-Jul-2009	1-Jul-2012	1-Jul-2014	6.3.3
105i	Successor Product Available	May, 2006	NA	1-Jul-2009	1-Jul-2012	1-Jul-2014	6.3.3
50i	Successor Product Available	April, 2005	NA	31-Dec-2008	31-Dec-2011	31-Dec-2013	6.3.3
100i	Successor Product Available	September, 2002	NA	30-Apr-2006	30-Apr-2009	30-Apr-2011	6.3.3
500i	Successor Product Available	September, 2004	NA	31-Dec-2008	31-Dec-2011	31-Dec-2013	6.3.3

1. UTM-1 and Power-1 Last order date set to 9/30/2012 in all regions, Successor products available (new 2012 appliances)
2. The IP350, IP355, IP380, and IP385 went end-of-sale on 4/30/2006 in all regions except for North America due to the RoHS initiative. These products went end-of-sale in North America on 11/30/2006, and the listed end-of-support dates apply worldwide.
3. The IP2250 went end-of-sale on 5/31/2006 due to the RoHS initiative. Since this product is closely associated with the IP2255, which replaced it, the end-of-support date for the IP2250 was aligned with the IP2255.
4. The RoHS versions of the IP1220 and IP1260 series require a minimum of IPSO 3.8.1.
5. Support for NSAS a la carte licenses that were purchased to operate on IP Platforms will be supported until the last support date for SSL VPN Platforms, 6/30/2010, or the EOCS date of the IP Platform the license is operating on, whichever comes first.

* Appliances können bis zu 180 Tage nach dem End of Support Datum unter Hardware Support genommen werden

Professional Services

Maximaler Nutzwert aus Ihren Check Point-Lösungen dank Expertenunterstützung

ÜBERSICHT

Die Check Point Professional Services umfassen eine Reihe flexibler Angebote zur Unterstützung von Endanwendern bei Entwurf, Implementierung, Optimierung, Administration und Management von Check Point-Produkten. Zu den verfügbaren Dienstleistungen zählen die Entwicklung vor Ort, Projektmanagement, erweitertes Technical Account Management (TAM), JumpStart-/Upgrade-Unterstützung, Analyse der Bereitstellung, Security Assessment und kundenspezifische Schulungen.

VORTEILE

- Zielgerichteter weltweiter Support durch ortsansässige technische Experten
- Schutz Ihrer wertvollen Assets durch Maximierung von Sicherheit und Leistung Ihrer Check Point-Lösung
- Planbare, pünktliche und kostengünstige Implementierungen und Anpassungen von Check Point-Lösungen
- Expertenempfehlungen zur Verbesserung der Systemeffizienz und der Leistung Ihrer Systeme

LEISTUNGSMERKMALE

- Expertenanalysen zu gegenwärtigen und zukünftigen Netzwerkmodellen als Grundlage einer vollständigen Sicherheitslösung
- Vor-Ort-Unterstützung durch Check Point Certified Security Expert-Berater
- Bewährte Projektentwicklungs-, Management- und Implementierungsmethoden
- Implementierungspläne, die exakt auf die Umgebungen und Anforderungen des Kunden zugeschnitten sind
- Klare Kommunikation und gegenseitige Vereinbarung von Projektabschnitten und Leistungen
- Check Point Security Architecture Review bietet detaillierte Untersuchungen und Vorschläge für Sicherheitsverbesserungen
- Transfer von Wissen und Fähigkeiten zwischen unseren Experten und Ihren Mitarbeitern

INTERESSANT FÜR

- Check Point-Kunden, die gegenwärtig Check Point-Produkte einsetzen oder dies planen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Tiefenanalyse der Check Point-Implementierung durch Sicherheitsexperten von Check Point
- Identifizierung interner und externer Schwachpunkte
- Stellt sicher, dass Kunden den maximalen Nutzwert aus ihren Check Point-Lösungen ziehen

GESPRÄCHSEINSTIEG

- Ist Ihre Sicherheitsumgebung auf maximale Sicherheit, Leistung und Stabilität hin optimiert?
- Würden Sie von einem einzigen Ansprechpartner für Entwurf, Implementierung und Management Ihrer Check Point-Lösung profitieren?

Schulung und Zertifizierung

Schützen Sie Ihre Ressourcen mit den bewährten Fähigkeiten unserer zertifizierten Sicherheitsexperten Certified Security Professionals

ÜBERSICHT

Schulungen und Zertifizierungen vermitteln die technischen Fähigkeiten, die zur Implementierung, Verwaltung und zum Management von Check Point-Produkten erforderlich sind. Es können Zertifizierungen der Stufen Administrator, Experte und Master für die Themenbereiche Network Security, Managed Security und Endpoint Security erworben werden. Die Zertifizierungen umfassen technische Schulungen mit praktischen Übungsbeispielen aus dem realen Leben, die über ein globales Netzwerk autorisierter Schulungscenter durchgeführt werden. Die Zertifizierungsprüfungen können in den Vue-Testcentern auf der ganzen Welt abgelegt werden.

VIRTUAL CLASSROOM – DAS BESONDERE COMPUTERLINKS-ANGEBOT

Neben den regulären Check Point Trainings bietet die COMPUTERLINKS Ihnen eine besondere Form des Klassenzimmers, das Virtual Classroom Training:
Kernstück des V-CL bildet eine vollständig virtualisierte Klassenraumumgebung, in der die Teilnehmer ein sehr ähnliches Lernerlebnis erfahren, wie sie es aus der traditionellen Seminarraumumgebung in Klassenraum-Seminaren / Workshops kennen.
Besonders herauszustellen ist der direkte audiovisuelle Kontakt zum Trainer und anderen Teilnehmern. Die Ausführung praktischer Übungen in der V-CL REAL-LIFE Lab-Umgebung und die unmittelbare Unterstützung durch den Trainer während dieser Übungen stellen einen besonderen Mehrwert da. Und dies, obwohl die Teilnehmer viele hundert Kilometer voneinander entfernt, von unterschiedlichen Standorten am Training teilnehmen.
Mehr Infos unter: training@computerlinks.de oder Telefon: +49 89 93099168

VORTEILE

- Wertvolle Fähigkeiten im IT-Sicherheitsbereich reduzieren Ausfallzeiten und die Auswirkungen von Problemen
- Bewährtes Wissen zu Check Point-Lösungen schützt Ihre wertvollen Ressourcen und steigert den ROI
- Erweiterter Zugang zur SecureKnowledge-Datenbank bietet zeitsparenden, spezifischen Support
- Security Expert Newsletter-Abonnement – stets auf dem Laufenden über Veranstaltungen und Aktionen von Check Point

LEISTUNGSMERKMALE

- Praktische, unter Anleitung durchgeführte Kurse vermitteln alle Informationen, die zur Implementierung, Verwaltung und Optimierung von Check Point-Lösungen erforderlich sind
- Interaktive Laborübungen bieten umfassende Möglichkeiten zum Lernen anhand realer Beispiele und für die Zusammenarbeit mit anderen Sicherheitsexperten
- Die Mitgliedschaft in der technischen Online-Community von Check Point bietet Zugang zu erweiterten Produktinformationen, interaktiven Foren und Webinaren zu Best Practices
- Technische Schulungen können in Schulungsräumen oder als Online-Live-Veranstaltung durchgeführt werden

INTERESSANT FÜR

- Alle Check Point-Kunden und Sicherheitsexperten, die gegenwärtig Check Point-Produkte einsetzen oder dies planen

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Check Point Certified Security Administrators (CCSA) erzielen laut der Gehaltsumfrage 2008 des Certification Magazine ein bis zu 16 % höheres Einkommen als ihre Kollegen
- CIO sehen Check Point an erster Stelle der Liste erwünschter Fähigkeiten zum Thema Sicherheit
- Stellt sicher, dass Kunden maximalen Nutzwert aus ihren Check Point-Lösungen ziehen

GESPRÄCHSEINSTIEG

- Verfügen Sie über Sicherheitsexperten, die nach mehr Anerkennung und neuen Möglichkeiten streben? – Check Point-Zertifizierungen garantieren die Anerkennung von Fähigkeiten und Erfahrungen und verbessern sowohl die Verdienstmöglichkeiten als auch die beruflichen Entwicklungschancen
- Wollen Sie die Möglichkeiten zur Weiterbildung optimal nutzen und potenzielle Fehler reduzieren? – Die konzentrierten Schulungskurse unseres Netzwerks von Authorized Training Centern (ATC) bieten die Möglichkeit, Erfahrungen mit realen Systemen zu sammeln und in einer sicheren Umgebung zu lernen. Die Teilnehmer lernen schneller, behalten einen größeren Teil des Erlernten und vermeiden kostenintensive Fehler, die beim Lernen im laufenden Betrieb auftreten können
- Verlassen Sie sich auf interne technische Support-Mitarbeiter? – Schulungen und Zertifizierungen von Check Point stellen sicher, dass Ihre technischen Support-Mitarbeiter über aktuelles Wissen und die Fähigkeiten verfügen, die zur Installation, Konfiguration und Verwaltung von Check Point-Produkten bei höchster Sicherheit und Effizienz erforderlich sind

SmartOptimize

Optimieren Sie Ihre Check Point-Umgebung

ÜBERSICHT

SmartOptimize stellt eine umfassende Checkliste mit mehreren Punkten zur Verfügung, anhand der sich die Netzwerksicherheit und Leistung verbessern sowie das Risiko neuer Bedrohungen reduzieren lassen. Der Service ist in drei Stufen verfügbar: Basic, Premium und Onsite.

VORTEILE

Steigern Sie Leistung UND Sicherheit:

- Säubern, konsolidieren und optimieren Sie Ihre Regelbasis.
- Identifizieren Sie nicht-konforme Firewalls.
- Analysieren Sie die Performance-Auswirkungen durch die Check Point-Empfehlungen.

Minimieren Sie mit leistungsfähigen Analysetools in kürzester Zeit Sicherheitsrisiken:

- Ermitteln Sie unsichere Regeln, und ergreifen Sie umgehend Maßnahmen, um Risiken zu reduzieren.
- Analysieren Sie Ihr aktuelles Gesamtrisikoprofil.
- Bewerten Sie den Zustand Ihres Sicherheitssystems.

Verringern Sie Komplexität und optimieren Sie die Sicherheit:

- Analysieren Sie Festplatten- und RAM-Auslastung, Benutzerlimits, Anti-Spoofing, Stealth-Regeln und vieles mehr in einem Bericht.
- Schließen Sie Sicherheitslücken unmittelbar durch die schnellere Installation von Richtlinien.
- Erhöhen Sie Kapazitäten durch eine bessere Auslastung von Ressourcen.

LEISTUNGSMERKMALE

- Firewall Management Analyse
- Regelbasis- und Richtlinien-Optimierung
- Risikoanalyse für die Regelbasis
- Analyse von Protokollen

INTERESSANT FÜR

- Check Point-Kunden, die über mindestens drei Check Point-Gateways verfügen
- Alle vertikalen Märkte
- Netzwerk-/Sicherheitsadministratoren und Chief Security Officers
- Wichtigste Einflusspersonen: CIO, VP/ Director/Manager IT, IS, MIS, Desktop- und Netzwerkgruppen, Prüfer

WICHTIGSTE UNTERSCHEIDUNGSMERKMALE

- Tiefenanalyse der Check Point-Implementierung durch Sicherheitsexperten von Check Point
- Detaillierter Bericht mit klaren Handlungsempfehlungen zur Verbesserung der Sicherheit, Leistung und Stabilität
- Persönliche Überprüfung zusammen mit einem Check Point-Sicherheitsexperten

GESPRÄCHSEINSTIEG

- Wissen Sie, ob Ihre Sicherheitsmaßnahmen gegenwärtig im Hinblick auf maximale Sicherheit, Leistung und Stabilität optimiert sind?
- Angesichts der Häufigkeit, mit der in den meisten Netzwerken Änderungen durchgeführt werden (neue Protokolle und Anwendungen, Richtlinien, Patches usw.), können Sicherheitsmaßnahmen, die bei der ursprünglichen Implementierung optimal waren, mit der Zeit an Wirksamkeit verlieren. SmartOptimize bietet eine gründliche Analyse der Check Point-Implementierung im Unternehmen und gibt Empfehlungen zur Optimierung der Sicherheit, Leistung und Stabilität

CHECK POINT APPLIANCE SUPPORT TIMELINE

Leistungsmerkmale	SmartOptimize	SmartOptimize Premium	SmartOptimize Premium Onsite
Optimierung der Regelbasis	■	■	■
Richtlinienoptimierung mit SecureXL	■	■	■
Optimierung von Datenbankobjekten	■	■	■
Stealth- und Säuberungsregeln	■	■	■
Anti-Spoofing bei Gateways	■	■	■
Systemzustand	■	■	■
IPS-Schutzübersicht	nicht verfügbar	■	■
Analyse protokollierter Regeln	nicht verfügbar	■	■
Onsite-Optimierung	nicht verfügbar	nicht verfügbar	■
Artikelnummer	CPTS-PRO-OPTIMIZE	CPTS-PRO-OPTIMIZE-PRM	CPTS-PRO-OPTIMIZE-ONSITE

Sie haben Fragen zu Check Point?
Rufen Sie uns doch an
Tel. +49 89 930 99 0

Oder senden Sie uns
eine E-Mail:
checkpoint@computerlinks.de
http://www.computelinks.de

COMPUTERLINKS
NEXT GENERATION DISTRIBUTION

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

©2012 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management,Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Oktober 30, 2012